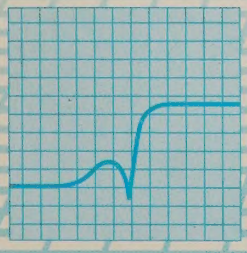
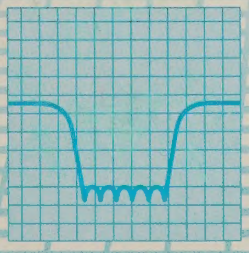
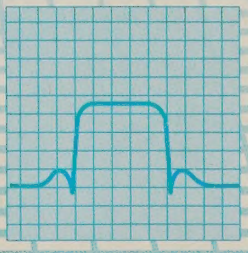
CATV Trapping

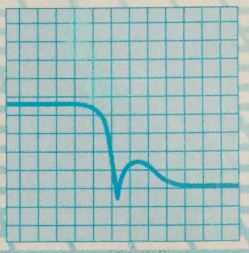
Security Filtering for Pay Television

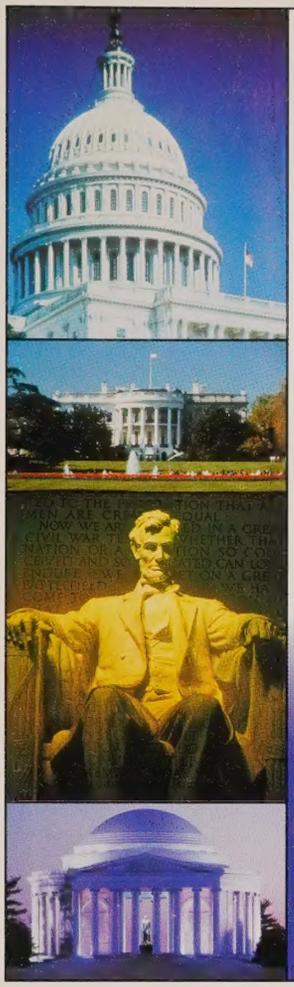
by Glyn Bostick, Emily Bostick & Ronald E. Mohar











SCBA

Small Cable Business Association

A Strong Voice For Small Cable System Operators

Call or write for information:
100 Greentree Commons
381 Mansfield Avenue
Pittsburgh, PA 15220-2751
412-937-0099 Office
412-937-0098 Fax

EPNY

The Pressroom of the Communications Industry

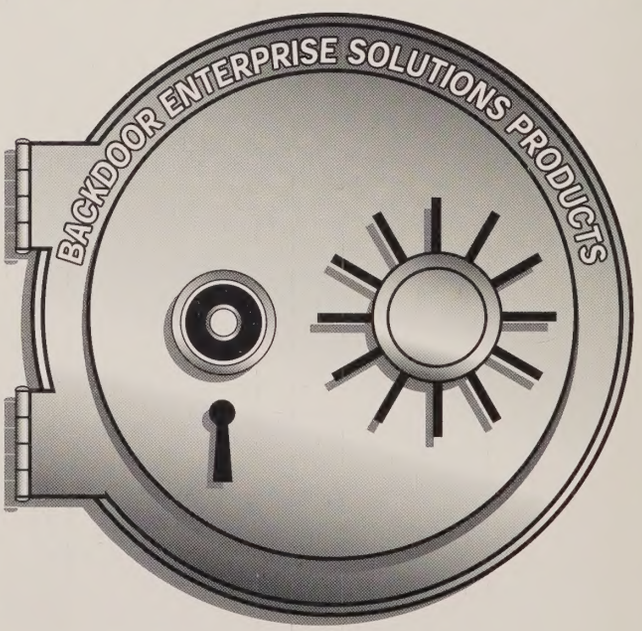
What is EPNY? We're printers- short run 4-color process is our specialty. We're publishers- our in-house team can write, lay out, illustrate and print your next publication.

Our in-depth knowledge of the communications industry is on your side whether you're a marketing manager, manufacturer's rep or self-publisher. Call us to assist you in getting your next important project in print.

Daniel Bostick
VP / General Manager
(315)452-5488 ext 2
Fax (315)452-5850
Email: dan@epny.com

EPNY
a division of C&E Corp.
7399 Taft Park Drive
East Syracuse NY 13057
USA

When it Should Look Like This..



...Reduce signal theft
...Increase Subscriber Count
...Increase Revenue
...Protect your Revenue Strea

We've made closing the Backdoor on Cable Theft Even Eas
Monitor 3.7 Coming Soon!

BACKDOOR®

(415) 634-0200
(414) 241-3037

CATV "TRAPPING"

Security Filtering For Pay Television

By Glyn Bostick, Emily Bostick, & Ronald E. Mohar

The Electric Press
A Division of the Communications & Energy Corporation
East Syracuse, New York 13057

ISBN: 1-888552-07-7

Library of Congress Card Catalog Number: 97-060597

© 1997 by the Electric Press
A Division of the Communications & Energy Corporation

All rights reserved under International and Pan-American Copyright Conventions. No part of this book may be reproduced in any form or by any means without the express written permission of the publisher. This includes photocopying, electronic or mechanical means, or by means of any data storage and retrieval system. No patent liability is assumed with respect to the use of the information contained in this book. While the authors and publishers have taken every precaution in the preparation of this book, they cannot assume any liability for errors or omissions. Neither is any liability assumed for damages resulting from the use of this information. The copyright claimed is exclusive of material from U.S. Government Documents.

The Electric Press
A Division of the Communications & Energy Corporation
East Syracuse, New York 13057

Acknowledgments

President . . . . . Emily Bostick
Executive Vice-President . . . . . Glyn Bostick
Vice President of Publishing Operations . . . . . Dan Bostick

Cover Design . . . . . Jerry Russell, Studio 309
Field & Studio Photography . . . . . R.E. Mohar
Illustrations . . . . . Sherri Stratton
. . . . . R.E. Mohar
. . . . . John Greatrex
. . . . . Janine Bostick
Illustrative Art . . . . . Sherri Stratton
. . . . . Christopher Bostick
Illustrative Models . . . . . Christopher Bostick
. . . . . Ernest Bottino
. . . . . Arcom Labs
Laboratory Research . . . . . Glyn Bostick
. . . . . Steve Shafer
Layout . . . . . Sherri Stratton
. . . . . R.E. Mohar
Library Research . . . . . R.E. Mohar
. . . . . Glyn Bostick
Prepress . . . . . Sherri Stratton
Printing . . . . . Lyle Priest
. . . . . Charles Teller
Proof Reading . . . . . Dave Bostick
. . . . . Sherri Stratton
. . . . . Michelle Wheeler-Dine
Technical Writing . . . . . R.E. Mohar

Some of the history contained in this book was derived from interviews by R.E. Mohar with Andy Tresness, Bernard Hitchcock, and Marty Zelenz. We deeply appreciate the help of Greg Tresness who read the manuscript for this book. Sherri Stratton's endless patience in revising this book is deeply appreciated. The authors wish to express their thanks to the following individuals for all of their assistance: Andy Tresness, Greg Tresness, Dave Deyo, Terry Sardella, and Marty Zelenz of *Arcom Laboratories*; Chandra Cornelison of *Home Box Office*, Rich D'Amato of the *National Cable Television Association*; Bob Portmess of *Eagle Comtronics*, and Rick Fleming and Louis Miceli of *Rent-a-Tech*. Karl W. Graverson, who drafted design diagrams for a number of urban CATV systems was of great help. Vince Cupples, who worked for a number of major cable systems and CATV manufacturers, assisted in a variety of ways. The following organizations were of help in writing this book : *Adelphia Cable Systems, Arcom Laboratories*, *Eagle Comtronics*, *General Instruments Corporation (Jerrold), Home Box Office*, the *National Cable Television Association*, *Philips Broadband Networks, Rent-a-Tech Inc., Scientific Atlanta, Time-Warner Cable*, and the *Turner Broadcasting Company*. The authors appreciate the strong support of the advertisers who helped make this book possible.

Contents

Acknowledgements iii
Contents iv
Forward By Gregory Tresness, President of Arcom Laboratories viii
Preface By Glyn Bostick, Communications & Energy Corporation x

Chapter 1 The Origins of Pay Television 1

Early Television Broadcasting 1
Reception Problems 2
Early Cable Systems 2
Rural Cable Systems 2
Urban MATV Systems 3
The Satellite Revolution 4
The Growth of Cable Television 5
Program Security 10

Chapter 2 Program Security 11

Program Security Methods 11
Cryptographic Methods 11
Interdiction 14
Passive Filtering Methods 14
Evaluating Program Security Systems 15

Chapter 3 History of Pay Television Filtering 22

History 22
Design 24
Production 25
Quality Control 28
Filter Specifications 29
Classification 31
Performance Characteristics & Capabilities 31

Chapter 4 Negative Filtering 35

Key Specifications 35
Channel Traps 37
Tier Filters 39

Chapter 5 Positive Trapping 43

The Positive Security System 43
Pre-Emphasis Systems 45
Sideband Interdiction 46
The Gaussian System 47
The SAWDEC System 48
Positive Filters 50

Chapter 6 The Economics of Filtering 52

Tier Filtering vs. Set-Top Converters 53
Filtering & Set-Top Converters 54
Single Channel Trapping 57
Positive vs. Negative Traps 58
Traps & Tier Filters 60
The Cost of Piracy 61
Developing A Filtering Strategy 62

Chapter 7 System Planning 63

Tier Filtering 64
Traps & Tier Filters 65
Channel Traps 67
Set-Top Converters & Addressable Taps 68
General Guidelines 69

Chapter 8 Cable Piracy 72

Piracy Law 74
Types of Piracy 74
The Positive Piracy System 76
Using Filters To Limit Piracy 77
Strategic War Planning 78

Chapter 9 Tap Audits 80

Classification 80
Monitoring Strategy 81
Reporting, Enforcement, & Tracking 81
Statistical Methods 82
Procedural Audits 84
Special Audits 86

Chapter 10 Physical Security 89

Tap Security 89
Set-Top Security 90
Buildings & Vehicles 92
Internal & External Controls 92
Computer Security 94
Employee Screening 94

Chapter 11 Cryptographic Systems 96

Properties of A Good Cipher System 96
Rationale 97
Tempest 101

Chapter 12 Special Filters & Filtering Networks 103

Amplitude Equalizers 103
Ingress Interference 103
Ingress Suppression Filters 103
Special Networks 106

Appendices 112

Appendix A: Reference Tables 112

Table A.1 Coaxial Line Loss 112
Table A.2 Conversion Table 112
Table A.3 VHF Television Channels 113
Table A.4 UHF Television Channels 115
Table A.5 UHF Broadcast Channels 118
Table A-6 HRC Channels 120
Table A-7 FM Radio Channels 124

Appendix B: Engineering Formulas 125

Appendix C: World Wide Channel Formats 128

Table C-1 International Channel Format 128
Table C-2 International Television Formats 132

Appendix D: International TV Channels 138

Table D-1 Australian 138
Table D-2 British 139
Table D-3 Chinese (Mainland) 140
Table D-4 Eastern European 141
Table D-5 French 142
Table D-6 International CCIR 144
Table D-7 Irish 145
Table D-8 Italian 145
Table D-9 Japanese 146
Table D-10 Moroccan 147
Table D-11 New Zealand 148
Table D-12 Russian 149
Table D-13 South African 150
Table D-14 Western Europe 151

Appendix E: Suppliers of Products & Services 152

Appendix F: CATV Distributors 155

Technical Glossary 156

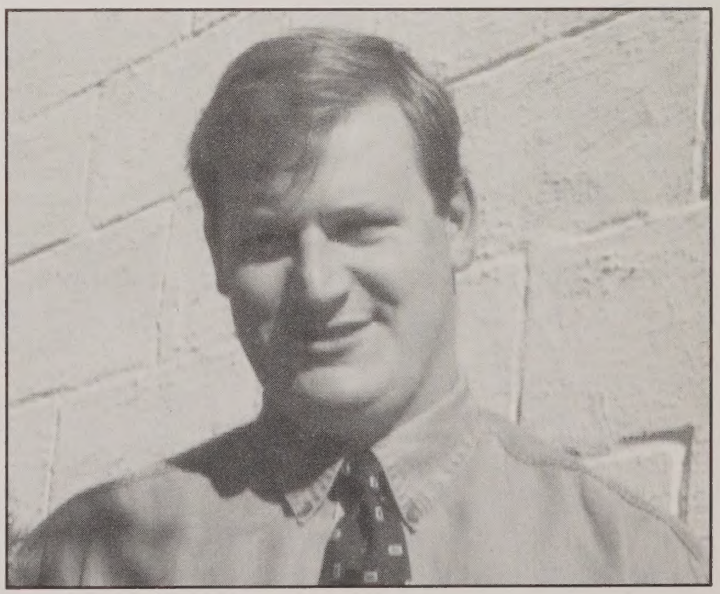
Forward

By Gregory A. Tresness
President, Arcom Laboratories

I am pleased to write a forward for this book as it is the first about traps and trap technology. I believe it will be a useful and informative source for anyone who has an interest in our industry. Sixteen years ago I got my start in the Cable Television trap and filter business in the factory of our family business. Today as I run our company I face many of the same challenges my father did twenty years ago. Our industry has survived and flourished despite predictions that the technology would never last.

The Cable Television business has gone through many cycles and trends over the years. In the quest to provide more channels, increase penetration, improve picture quality and ultimately increase revenue, many approaches, product mixes, and methodologies have been tried. One of the areas where much effort has been spent is that pertaining to how to most efficiently and economically segment services: i.e. basic, extended basis, pay channels, and pay-per-view. Traps provide an important contribution to this puzzle. I am continually asked questions along the lines of - "Are people still using traps?" Over the last ten years my answer has been the same, and it is still true today. Yes, traps still enjoy widespread usage in the United States and throughout the world. Certainly traps are not the solution 100% of the time for every operator in every situation, but I firmly believe that every single operator or system has some use for traps and filters. These applications may range from using a negative trap on one or two high penetration pay services, to provide a 'lifeline basic' or extended basic package, to offer a few low penetration niche pay channels, or simply to remove pay programming from bars. There is widespread misunderstanding throughout the world on where and how traps can be used. The most common misconception is that different security methods are mutually exclusive; that a system which uses addressability can and must only use addressability. The most efficient method to segment pay channels, basic packages, and PPV is in all likelihood a mix of several technologies. A very commonly used approach is to use negative traps on the one or two most popular channels, use tier traps to segment basic and extended basic, and use addressable converters for additional lower penetration pay services and pay per view. Looking to the future, the same mix of security technology described above could also be used in conjunction with a digital tier using the new compression boxes. The digital tier would be placed above the analog offerings, all on the same cable system. In the United States, Home Box Office is the most successful pay channel. This success can in part be attributed to the fact that most systems negative trap HBO and do not use a set-top box for security. The ability of a subscriber to get HBO without the box is a big selling point and a competitive advantage for HBO.

Every time a new technology in the area of signal security comes along there are some people who say that this will be the end of traps. Although we constantly watch new developments we have been hearing this for almost twenty years and now take it with some degree of skepticism. First came programmable descramblers, then came sync suppression addressability, then came improved sync suppression addressability, then base-band converters, then interdiction, and now digital compression. These are all or were all good technologies, but they each have their benefits and pitfalls and are not necessarily appropriate for every application. Like traps each of them has situations where it makes sense to deploy,



and situations where it doesn't. There have been and continue to be many operators who try to go one way and remove all of the traps from their system when they implement one of these technologies. The pay channel penetration and cash flow ultimately suffer and frequently operators go back and re-install the traps they have removed, settling for a mix of technology. If for example you have a subscriber whom only wants basic and one pay channel, and doesn't care about anything else, it is an inefficient use of valuable resources to install a $150.00 addressable converter when the same function can be achieved using $ 4.00 negative traps.

When traps first appeared about twenty years ago, they were used to provide security for HBO. Both HBO and the operators profited, and new opportunities were created. Traps provided the programming security which initially got the pay television business started. As the business grew it was evident that there was demand for additional pay programming. The operators grew into the business by gradually increasing their programming offerings as they could afford to, and as customer demand warranted. In many areas of the world in which cable is fairly new, I feel it is a mistake that operators do not learn from this. They frequently try to jump right into a higher technology like addressability, which they may not be able to afford, rather than to start slowly and offer only a few pay channels using traps as the initial security. After the operator has had some successes and has learned how to effectively market their services, they can then look at offering more services which could necessitate supplementing the traps with a technology such as addressability.

New advances and major improvements in technology have again put traps ahead on the value curve. In the past positive traps were by far the most economical method of securing low penetration pay channels. However, they were not without some faults. Security and picture quality were always suspect. Great amounts of research and development capital have been spent in the last few years and a major result is SAWDEC, which is a technology that improves upon and replaces positive traps. SAWDEC is as economical as the old positive trap technology. However, both the security and picture quality are remarkable. The economic advantage remains yet the negative points on picture quality and security have been eliminated.

Another new and important use for a trap has recently emerged. Business opportunities in telephone, data, and Internet access have necessitated use of the two way capabilities in the cable plant. In order to effectively, accurately, and reliably transmit data from the home at high speed, filters are required in varying degrees. Dozens of system operators are experimenting and learning what is necessary to make two way transmissions work effectively. The early results point to the need for subscriber filters in order for the network and operator to be able to provide the type of reliability which the consumer demands. New products such as Step Attenuators and Windowed High Pass filters can help get this reliability where it needs to be.

One of the biggest challenges the trap and filter industry faces is explaining how all of our products can be used efficiently and effectively to maximize revenue for the system operator. It is my hope that this book will assist in these efforts, communicate useful information, and ultimately result in system operators benefiting from our technology.

Preface

By Glyn Bostick

Communications & Energy Corporation

The first cable systems charged subscribers one fee and gave them access to all channels on the network. These universal channels became known as "basic" channels. In the mid-1970s premium entertainment , such as movie channels and major sports entertainment, was introduced on special channels. Subscribers who wished to view them paid an additional fee. Therefore, there was an immediate need for a security system to prevent unauthorized viewing of these special channels by subscribers who had only paid for basic service. "Trapping" was the first security system introduced to meet this need.

"Trapping" is the practice of inserting an electronic filter into the subscriber's drop-line to block premium channels from reaching the subscriber's television set. For several decades it has been predicted that "tapping" would become obsolete due to the introduction of addressable (computer controlled) set-top converters. However, due to the *inherent flaws* of *cryptographically protected program security systems* and the high expense of security systems based upon "interdiction," the predicted obsolescence of security filtering has *failed to materialize.* Meanwhile, the pages of the major trade publications continue to document major cable piracy cases involving the distribution of pirate set-top converters, "decoders," and cryptographic processing chips. Worse still, *pirate decoders are very difficult to detect in the customer's home.* Cable operators who are heavily invested in specific decoder systems which have been "broken" find themselves with mysteriously declining subscription rates at exactly the time they need to reinvest in new equipment. In fact, *some cable operators have actually begun to pull set-top converters out of most subscribers' homes.*

Today, negative "trapping" remains the single most secure and economical program security method available. This is true because *the only sure way* of protecting signals from piracy is to prevent them from entering the subscriber's home. Once the subscriber has the signals necessary to make an intelligible picture, it is possible to find a way to do that. However, if drop-line piracy occurs, negative "trapping" makes the piracy *detectable* and *prosecutable.* This simplicity and affordability have been the keys to the survival of "trapping" as a program security strategy.

The only significant costs associated with "trapping" are the cost of the filters, the cost of installation, and the cost of periodic drop-line audits. A choice of two different major schemes is available. Where demand for a particular channel or group of channels is high, only a few negative filters are required. Where demand is low, only a few positive filters are required. Another major advantage of filtering is that the scheme is *user friendly.* "Traps" do not place constraints on "cable compatible" television sets and VCRs. Nor do they duplicate receiver circuitry already in the consumer's home. Finally, filtering offers operators a method of enhancing the security provided by set-top security systems.

In contrast, the cost of addressable converters or taps is high. Sophisticated set-tops and addressable taps malfunction periodically and require maintenance. Set-top converters place constraints on subscriber's television sets and VCRs while unnecessarily duplicating receiver circuits already in the consumer's equipment. Set-tops also create an unnecessary expense for subscribers who have more than one television in their home. While addressable set-top converters will probably continue to have applications with customers who take a large number of premium channels, more and more operators are seriously re-evaluating the way in which they deploy their set-top converters.

DEDICATION

GLYN BOSTICK (1923 - 1997)

On August 28, 1997, while this book was going to press, Glyn Bostick passed away in DeWitt, New York, after a short illness, surrounded by his family. Although Glyn was working on a number of different manuscripts, for more than a decade he always wanted to write a book on "Pay Television Trapping." He spent months collecting background material and writing cryptic notes during the evening before the first draft of this book was written.

Glyn was a romantic engineer. He loved talking directly with customers and being able to help them solve their problems. He sometimes used to design new filters for his customers while talking with them on the phone. He once said; "For me, all of these years, the romance has never gone out of it. Hearing a worried voice in the night from thousands of miles away and being able to help the guy has never lost its romance."

Glyn was a workaholic who loved his work and *had an answer for everything*. He frequently put in twelve hour days, seven days a week. He was not afraid of death. He only worried that his family, friends, associates, and customers would miss him and he didn't like the idea of not being able to design filters and antennas anymore. Glyn used to say that he didn't sell "stuff," he sold remedies. "A filter is like medicine - it comes with the remedy." He used to show his associates product files on various filters and tell them that he was fully documenting everything he did so that other engineers could follow his design calculations and figure out how he arrived at various answers. It remains for his disciples to continue his work.

Chapter 1
The Origins Of Pay Television

From the beginning, cable television was an outgrowth of television broadcasting. "*Subscription television*" (STV) or "*pay television*" (PTV) began in the United States with cable television systems intended to supply service in poor reception areas. Although pay broadcast television exists in many other countries, American PTV was an outgrowth of "free" *commercial television* (CTV). Because cable systems require revenue to pay for installations, infrastructure, and maintenance cable television is *inherently* a pay television service. It took around twenty-two years for the cable industry to establish its first 2,500 systems. Yet between 1980 and 1982 the cable industry started to grow at a more rapid rate as cable spread to metropolitan areas throughout the country. Between 1970 and 1994 the number of cable systems in the United States grew from approximately 2,490 systems to more than 11,217 systems.

Early Television Broadcasting

Although rudimentary televisions appeared in the laboratory during the 1920s, the first experimental broadcast stations were established by RCA and CBS during the 1930s. RCA began experimental field testing at UHF frequencies with broadcasts from the *Empire State Building* in 1936. The first two commercial stations (WNBT and WCBW) licensed in New York City began regular operation on July 1, 1941. When restrictions ended following the Second World War, the television industry grew more rapidly. In 1948 there were only sixty television stations with one million receivers in the United States. Yet by 1951 some *ten million* television receivers had been sold.

When American television broadcasting began in the mid-1940s building a television station was a risky business. Television was an entirely new technology. The first experimental stations were financed by large radio networks because only large corporations could afford the costs. The technology was entirely new. Entrepreneurs faced the problem of how to finance a station. There were two possibilities - *commercial television* (CTV) or *pay television* (PTV).

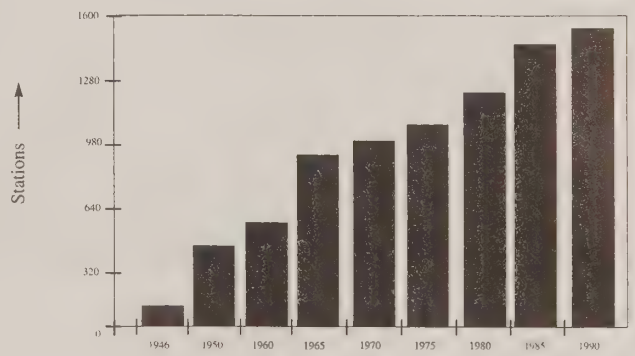
Early broadcasters decided that "free" *commercial television* was most likely to promote rapid development. Because television sets were relatively costly, it was unlikely that prospective viewers would buy a television and then pay a subscription fee on top of the first expense. Since broadcasters were licensed to use public frequencies, there was little if any justification for charging viewers to watch programming on their own frequencies. Finally, commercial radio had already established a precedent. Viewers expected "free" television service. Hence, most stations began as commercial enterprises. In fact, when WNBT began broadcasting in New York, it had four commercial sponsors.

Commercial television depended exclusively upon advertising revenue. But the value of advertising depended upon the number of viewers watching it. Who is going to pay for advertising with no one watching? Without a television station, there was no reason for someone to buy a television set. But without television viewers, there was no reason to set up a station. Thus, establishing a television station required a "leap of faith." It also required large capital investments over a period of time before significant revenue started flowing.

Early television broadcasters learned a lot from radio broadcasting. Three significant factors prompted them to establish their ventures near large population centers. First, more people were likely to

NUMBER OF VHF/UHF TV STATIONS

Figure 1.1



own or buy television sets in cities. Second, given a fixed transmitter output, it was possible to reach more people near large population centers. Finally, because television stations depended upon advertising revenue, more viewers increased the value of a station's advertising. Hence, early television stations were always established near large cities like New York or Philadelphia.

Reception Problems

The success of television broadcasting in large cities lowered the perceptual risk of launching a station. Eventually, television came to medium and small cities. However, small towns and rural areas were left out. Because television depended exclusively upon advertising revenue, there was little incentive for entrepreneurs to establish stations near small towns or in rural areas. Such communities were either left without service or had poor reception from large regional stations.

Unlike lower frequency radio signals, VHF television signals tend to follow a direct line-of-sight between the broadcast and reception antennas. Although there is some signal bending at VHF frequencies, any serious blockage between the transmitter and receiver can degrade or block reception entirely.

Early Cable Systems

Cable television systems were established to solve reception problems. Although it is generally agreed that the first American "cable systems" were set up in 1948, there is some dispute as to which system was "first."[1] In June 1948 John Watson set up a system in Mahanoy City, Pennsylvania. Watson connected a pole mounted antenna on a hill to a warehouse at the bottom of the hill using 300-ohm twin lead. On November 28, 1948 Ed Parson used a coaxial cable to carry signals from the roof of the Astoria Hotel in Astoria, Oregon to his apartment across the street. Both eventually got into the cable business.

In many areas of Pennsylvania the terrain is hilly and mountainous. (Photo by C&E Corp.)

Rural Cable Systems. The first cable systems were usually established in rural areas to bring television to communities where reception was blocked by hills or mountains. They were relatively simple systems devised by local technicians to serve only a few homes. In those days a few homes were simply wired to a master antenna equipped with a booster amp using either coaxial cable or 300-ohm twin lead.

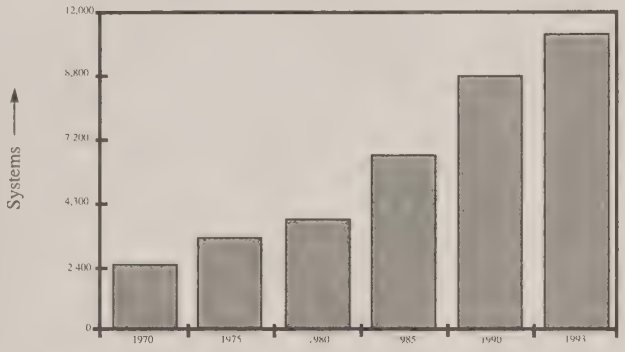
Typically the community was located in a valley where there was little if any television reception. An antenna was usually located above the valley on a hill. Because a higher antenna increases the "radio reception horizon," it usually received stronger signals. Thus, antennas were frequently mounted atop towers or tall structures to increase their height. A booster amplifier was often connected to the antenna to increase signal levels. Today, this first amplifier is called a "*launch amplifier*." A cable, connected to the amplifier, was run down the hill to homes located in the valley. This main cable later became known as a "*trunk cable*" or "*trunk line*."

On passing a home, a smaller cable would be attached between the trunk line and the home. This

[1]In 1926 Professor Louis H. Cook (1888-1953) applied for a Patent entitled "Non-Grounded Transmission Line." The Patent (No. 1,645,643) was issued on October 18, 1927. Professor Cook filed another Patent, entitled "[A] System and Method for Sending Pictures Over Telephone Wires," on November 18, 1937. That Patent (No. 2,222,606) was issued on November 26, 1940. Some of the first experiments with cable television were carried out in England and Germany prior to the Second World War. In England the British Broadcasting Company (BBC) experimented using pairs of twisted wire to transmit television pictures to multiple receivers. They called this method "rediffusion." In Germany two parallel 90-ohm cables were used experimentally to wire buildings and groups of buildings for television.

NUMBER OF CATV SYSTEMS

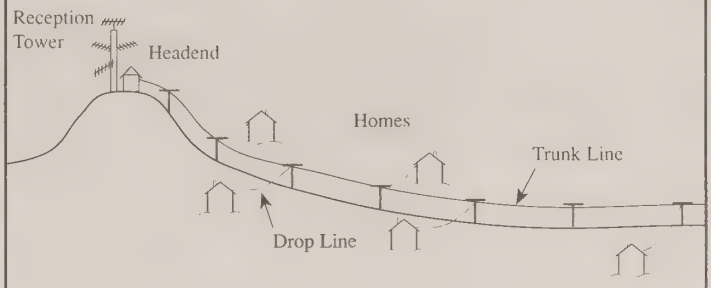
Figure 1.2



Source: NCTA, 1994

RUDIMENTARY CATV SYSTEM

Figure 1.3



smaller cable later became known as a "*subscriber drop cable*" or "*drop-line*." Such cable systems eventually became known as *Community Antenna Television* (CATV) systems because a number of individual homes all shared the same reception antenna. Since small cable systems did not require full time staffing and because programming was "free" to the cable operator, the fee charged subscribers could be kept relatively low. Because CATV systems crossed public right of ways, they quickly came under public jurisdiction. Thus, cable systems are regulated today at the federal, state, and local levels.

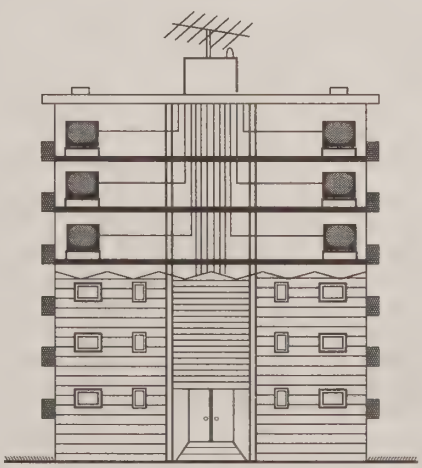
Urban MATV Systems. Rural viewers were not the only populations with reception problems. The Waldorf-Astoria Hotel in New York City had a *Master Antenna Television* (MATV) *system* as early as 1949. Some urban viewers relied upon a simple set of "rabbit ears" for receiving pictures. Rabbit ears were sufficient for good reception in strong signal areas. But reception was not always good in large apartment buildings where the structure of the building itself sometimes blocked signals. Viewers in single family homes could simply purchase a roof-top antenna and set it up. But in large apartment buildings, use of separate roof antennas for each apartment created a "jungle." In cities with tall skyscrapers, large buildings could also block reception or create unsightly ghosts in pictures.

In large apartment buildings, a separate antenna for each apartment can create some problems. When several antennas are located in close proximity, they can interfere with each other. "Antenna coupling" can change the normal reception patterns of the individual antennas. Routing separate cables between each apartment and its antenna results in a tangle of wires down the side of the building. Finally, the aggregate cost of separate antennas for each apartment is higher than that of a professional MATV system.

MATV systems were designed to solve reception

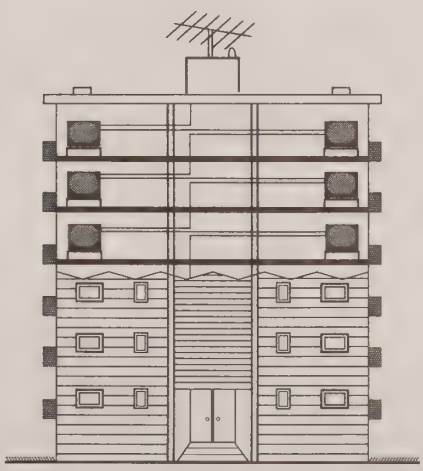
HOME RUN MATV SYSTEM

Figure 1.4



LOOP RUN MATV SYSTEM

Figure 1.5



problems for urban viewers in apartments. A roof antenna was simply connected to a distribution amplifier. A cable distribution network was then used to interconnect each apartment with the roof antenna. Two different types of distribution systems evolved - (1) *home run systems*, and (2) *loop run systems*. A "home run" system uses a separate cable from a central distribution amplifier to each apartment. A "loop run" system uses a single cable for the whole building. In a loop run system, an impedance matching network is used to connect the cable to each apartment. Although loop run systems are less expensive than home run systems, they are more difficult to design, balance, and troubleshoot. Although home run systems are easier to design and troubleshoot, they are also more costly.

Because MATV systems seldom crossed public right of ways, it took longer for regulators at the federal, state, and local levels to promulgate relevant regulations. Thus, MATV systems eventually became known as "private cable systems."

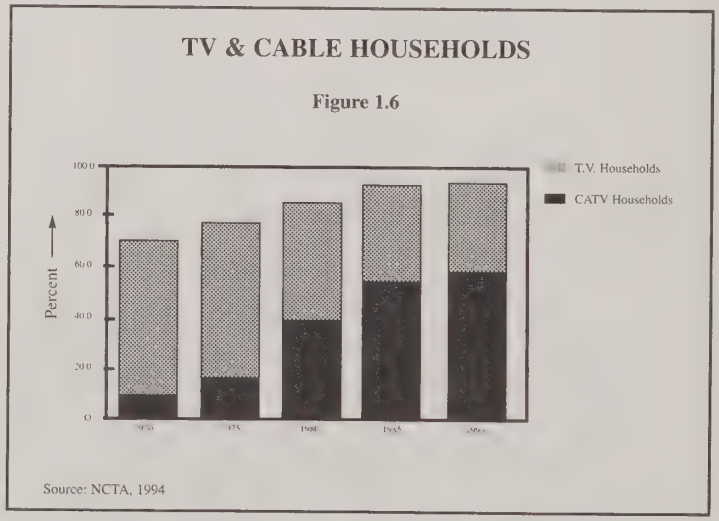
The Satellite Revolution

Satellite broadcasting revolutionized the cable television industry. The success of cable in rural America demonstrated that viewers would pay for television service if it improved their reception or provided unique entertainment which was not available over-the-air. By 1970 there were approximately 2,460 cable systems in the United States serving 5.4-million subscribers. Compared with 93-million television sets, cable television represented only 5.8-percent of the national television market. Thus, prior to the satellite revolution, cable television represented a small "niche market" in isolated communities which could not receive signals.

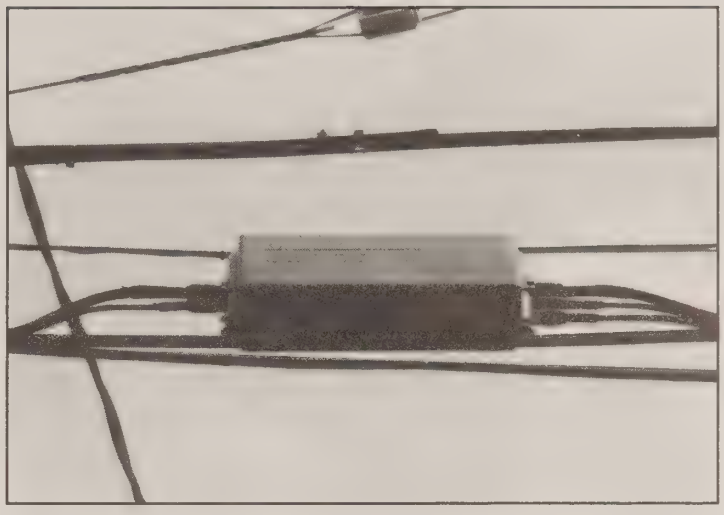
During the 1970s things began to change. A relatively small division of *Time Inc.* - called *Home Box Office* (HBO) - began transmitting programming to just three-hundred sixty-five subscribers of *Service Electric Cable Television* in Wilkes-Barre, Pennsylvania via AT&T's terrestrial microwave network. Although satellites had been used by the networks to relay short duration trans-Atlantic television broadcasts, no one had ever used satellites to *distribute* domestic broadcasting. *Television Receive Only* (TVRO) earth stations were large and relatively expensive. Hence, satellite broadcasting was thought to be too expensive and too technical for routine use.

On September 30, 1975 HBO introduced an innovation which profoundly influenced the whole television industry. Although the broadcast was experimental, HBO became the first organization to use a *satellite* to distribute their programming.

By December 10, 1976 HBO obtained permission from the *Federal Communications Commission* (FCC) to use an inexpensive 4.5-meter TVRO dish for program reception. By dramatically lowering distribution costs, it became possible to distribute signals to every cable system in the country. Seven days later - on December 17, 1976 - Ted Turner began beaming "Superstation" WTBS from Atlanta to cable systems all over the country on Satcom III-R. Within one year WTBS grew from 694,746 households to more than 1.9-million households. By 1980 Turner's "Superstation" was connected to 13.2-million households. As a result of these successes, Turner



HBO revolutionized the broadcast industry by introducing satellite distribution of programming. Their first broadcast was to Service Electric Cable System in Wilkes-Barre, PA via AT&T Microwave. (Photo by C&E Corp.)



Typical Jerrold CATV Line Amplifier. (Photo by C&E Corp.)

introduced a 24-hour news service called *Cable News Network* (CNN) in June 1980. This was followed in January 1982 by the introduction of a second 24-hour news channel called *CNN Headline News.* CNN focused on "in depth news." Unlike CNN, Headline News repeated a 30-minute broadcast every half-hour. The success of channels like HBO, Cinemax, CNN, and CNN Headline News produced an avalanche of specialized programming designed to appeal to every niche market imaginable. Thus, the stage was set for the introduction of financially viable urban cable systems.

The Growth of Cable Television

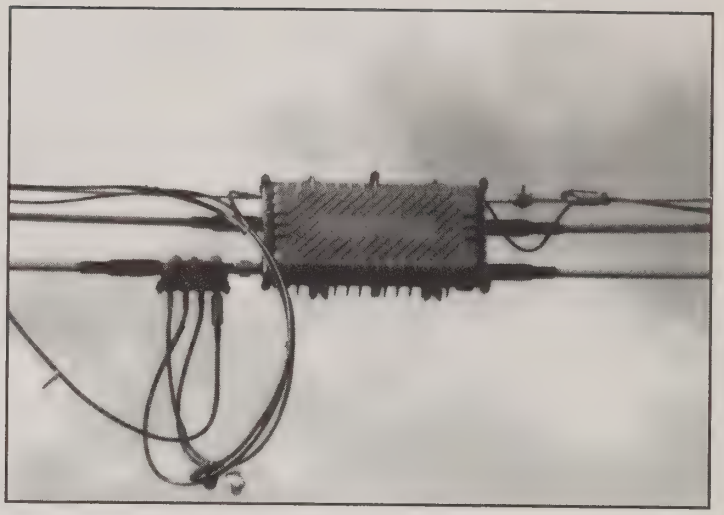
Prior to the "satellite revolution," most cable systems had sufficient spectrum to carry twenty VHF television channels. However, until the introduction of satellite broadcasting most of this spectrum capacity was not used. Before satellite broadcasting most cable systems served to simply extend the reach of broadcast stations. Without an inexpensive menu of unique entertainment, most systems lacked sufficient programming to fill available spectrums. Hence, without unique programming, urban cable systems in "good reception" areas didn't make much financial sense. Who was going to pay to receive channels which they could get free by simply setting up a roof antenna?

Since television broadcasting was dominated by the "big three" television networks (ABC, CBS, and NBC) an urban cable system was more or less limited to local network affiliates. Although a system could supplement local channels with "imported" broadcasts from other cities, most out-of-town stations were usually affiliates of the same "big three" networks. Although network affiliates regularly received programming via AT&T microwave, individual long-distance microwave feeds were too expensive for most small cable systems.

The situation changed when satellite programming became available. Suddenly urban cable systems in "good reception areas" made financial sense. Because the number of households passed by a cable was greater in urban areas, laying cable was less expensive. Where a rural system might have to lay a mile of cable to pass a few homes, some urban systems might pass several hundred households in high rise buildings along one city block. Eventually urban systems became quite complex. Typically trunk lines would be run down main streets with feeder lines run down the side streets. Trunk lines and feeder lines were usually 1/4-inch, 1/2-inch, or 3/4-inch coaxial cable.

Directional couplers were used to tap signals off the cable. The directional couplers fed either six-way or eight-way power splitters serving homes in the vicinity of the tap. For simplicity and reliability the directional couplers and power splitters were usually integrated into a single weatherproof housing. Either RG-59 or RG-6 coaxial cable was usually used on drop-lines.

A typical CATV power unit (Photo by C&E Corp.)



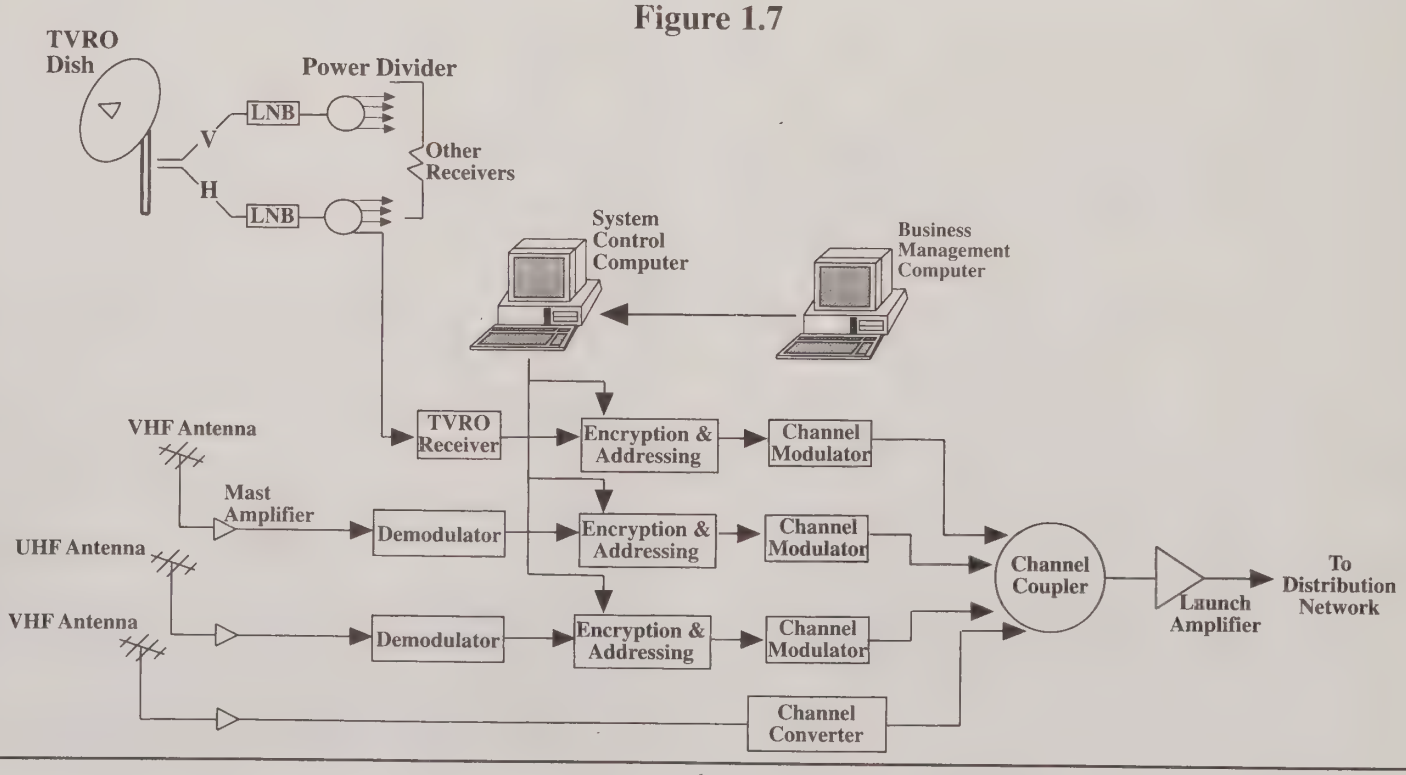
Typical Magnavox (Philips) CATV Line Amp with Taps (Photo by C&E Corp.)

Since cables were usually strung on utility poles underneath power lines and telephone lines, the network was powered by simply tapping into the power lines at periodic intervals. Thus, power supplies were located along the cable at periodic intervals. These power supplies usually placed 60 VAC onto the coaxial cable to power the line amplifiers. Each amplifier then converted the 60 VAC on the cable to DC.

Three different kinds of amplifiers evolved - the *trunk amplifier*, the *line extender*, and the *bridger amplifier*. *Trunk amplifiers* were designed for long hauls where "line-tilt" becomes a significant factor. Because the higher frequency channels tend to be attenuated more than lower frequency channels, channels which are launched at the same level do not

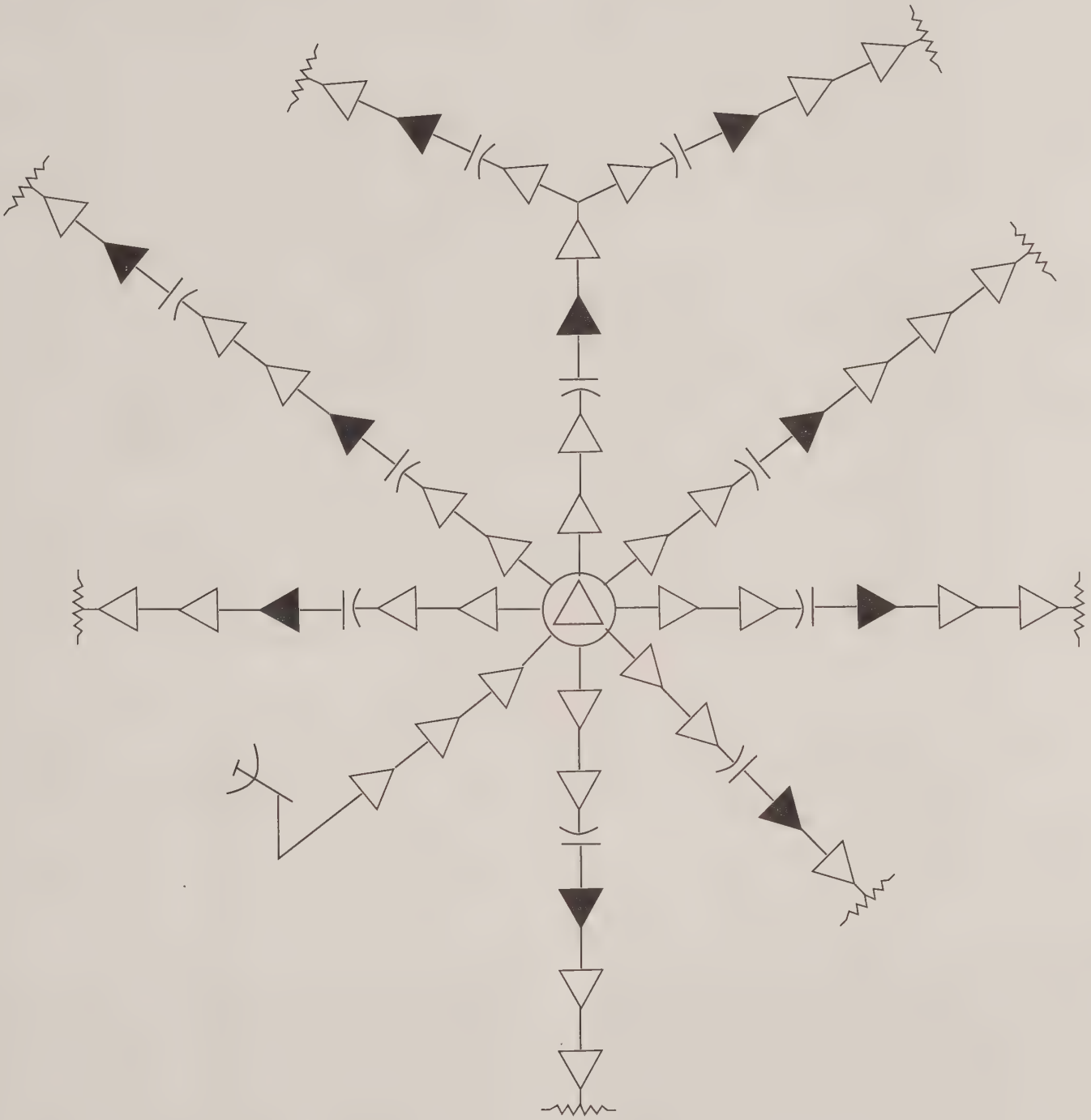
A CATV HEADEND

Figure 1.7



TYPICAL CATV SYSTEM

Figure 1.8



Legend

Amp with Power Supply

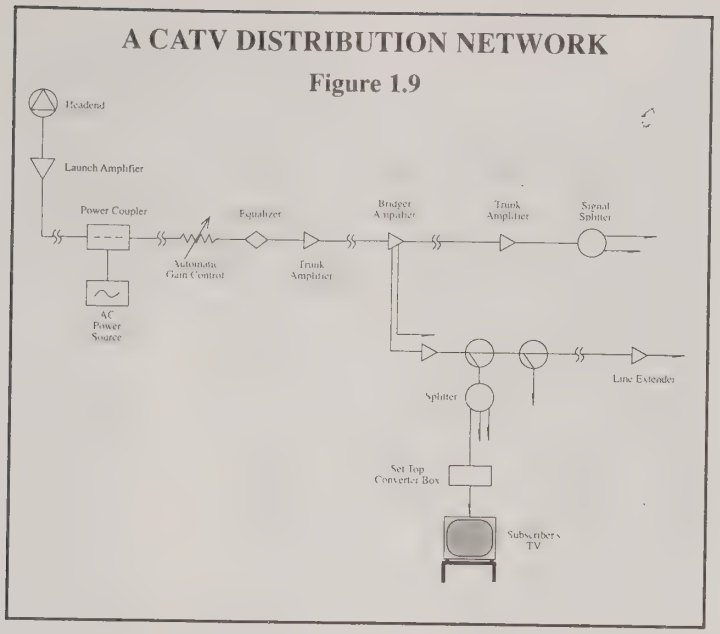
Amp without Power Supply

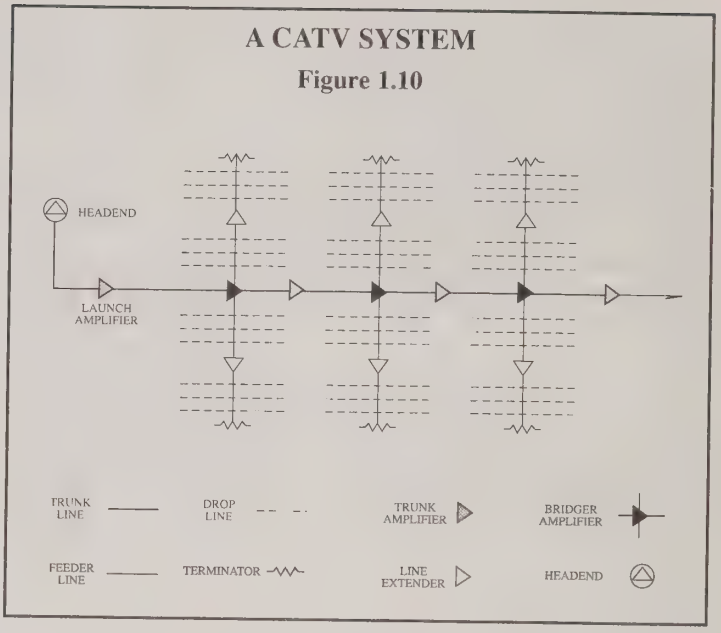
Power Stop

TVRO Dish

Terminator

Headend



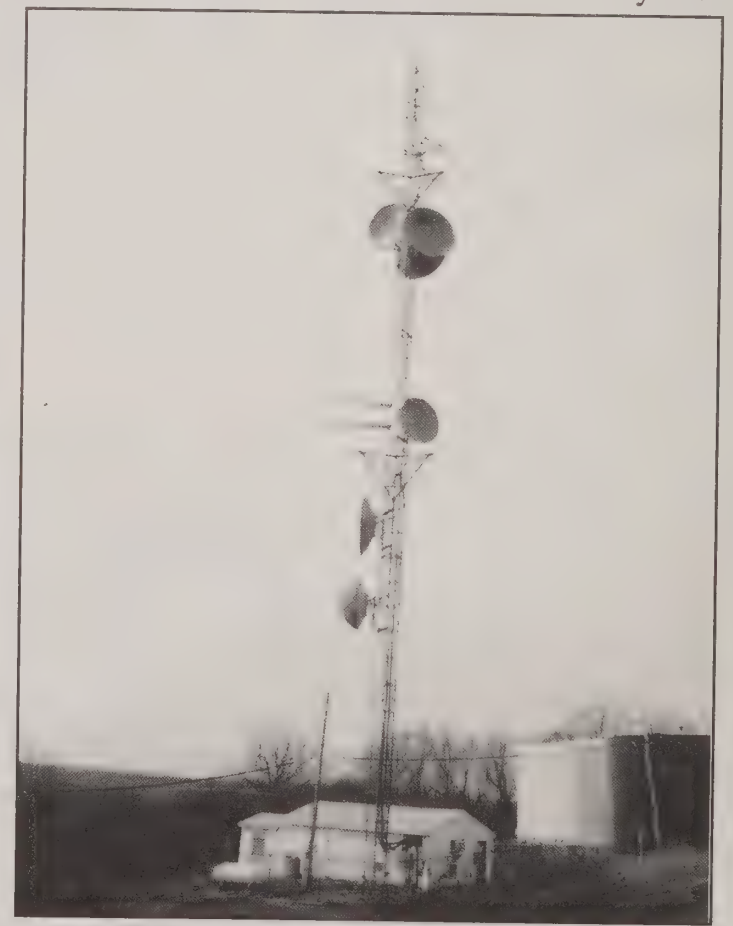


stay at the same level as they move along a long trunk line. Trunk amplifiers were usually equipped with *automatic gain control (AGC) circuits*, equalization circuits, and power supply circuits. Automatic equalization circuits - called *automatic slope controls* (ASCs) were eventually developed to compensate for "line-tilt." *Bridger amplifiers* were equipped with power splitters for supplying signals to feeder lines. *Line extenders* were simple short run amplifiers designed to boost gain along city streets where line-tilt is not a factor.

The satellite dish and any VHF/UHF reception antennas were located at what became known as the *"headend."* Some large cable systems had more than one headend for optimizing reception on specific channels. Remote headends were connected to the main headend using either a coaxial cable or a small microwave link. Such links later became known as the "*transportation system.*" Eventually some systems used these small *amplitude modulated microwave links (AMLs)* to import out-of-town channels.

Because standard television sets were only equipped to receive VHF Channels 2 to 13 and UHF Channels 14 to 83, the cable television industry had

A Time-Warner Headend near Syracuse, New York. (Photo by C&E Corp.)



A Time-Warner Headend Reception Tower near Syracuse, New York. (Photo by C&E Corp.)

to develop "set-top converters" for subscribers to receive twenty VHF channels. These devices were designed to convert any channel on the cable to either Channel Three or Four on the subscriber's television set. Thus, the subscriber's television was tuned to either Channel Three or Four and left there. Subscribers changed channels using the set-top converter.

Because the FCC does not license adjacent television channels in the same area, many television receivers during the 1950s, 1960s, and 1970s were more or less designed for *semi-adjacent channel operation*. Tuner circuitry was not very selective. Set-top converters were designed with highly selective tuners specifically intended for adjacent channel operation. Hence, set-tops sometimes improved receiver performance on the cable system.

To some extent early set-top converters allowed cable operators to perform a security function. By setting up a cable system with all the premium channels in the VHF mid-band (between VHF channels 6 and 7) an operator could equip only premium customers with converters. Of course, a television repairman could make a set-top converter capable of receiving mid-band channels using a modified television tuner from an old set. But for most subscribers, lack of a set-top converter was a serious obstacle. This kind of "program security" became completely ineffective when *generic* converters became available through electronics stores like the *Radio Shack*. Eventually, the set-top converter box served to house various *security devices* designed to limit the subscriber to only those channels which the subscriber was authorized to receive.

With the introduction of fiber optics, many cable operators are converting their trunk lines to fiber in order to increase their channel capacity. A single fiber has sufficient spectrum capacity to easily carry several CATV spectrums with room left over for hundreds of telephone channels. In place of a launch amplifier, fiber systems use an optical modulator to put signals onto the cable. A single fiber can transport signals virtually distortion free up to fifteen miles without any intermediate amplifiers.

Because it is seldom cost effective to string only one or two fibers, operators usually string a cable carrying at least fourteen fibers. Such a cable is usually about the size of an RG-6 coaxial line and has tremendous channel capacity. However, since optical systems are fragile and expensive, many continue to use coaxial feeder lines. For the same reason, many if not most continue to rely upon coaxial drop-lines. Optical receivers are used to demodulate signals for insertion onto coaxial feeder lines.

Between 1982 and 1991 the number of CATV systems in the United States grew from 4,825 to 10,704. By 1992 *sixty-one percent* of the households in the United States were connected to cable. As cable became more popular, television manufacturers began to design "*cable compatible*" television sets. These new sets were designed with tuners capable of receiving a hundred VHF/UHF channels or more. Thus, eventually set-top converters became unnecessary for basic subscribers. This reduced costs

Typical Set-Top Converter (Courtesy of Jerrold Communications)

Typical CATV Curb Pedestal (Photo by C&E Corp.)

for the cable operator since the only subscribers who needed a set-top were those who required it for premium reception.

Program Security

From the beginning, cable television systems had a "security problem." It was relatively easy for anyone along a cable route to simply climb a pole and connect up their own drop-line. Hence, cable operators had to inspect their lines periodically for "unauthorized taps." When rural systems were small this was relatively simple. A cable technician would simply compare the drop connections to a list of authorized subscribers. Along routes with single family homes unauthorized connections were relatively obvious.

As urban systems became larger and much more complex, such "audits" became a much more cumbersome process. In urban apartment buildings it is much more difficult to determine whether an illegal drop is connected into a line. Without access to a building, it is difficult if not impossible to determine whether an authorized subscriber is feeding signals to other unauthorized apartments.

When satellite programming became available, cable operators needed a means for separating "basic" subscribers from those who were paying for premium channels. Starting in the late 1970s a variety of methods were developed for securing selected cable channels. Although the cable industry has yet to develop an *infallible* security system, many of the methods developed provide sufficient security to deter the majority of cable "pirates." In general these methods may be divided into three broad categories. The first category involves the use of *passive filtering devices*. The second involves *cryptographic methods*. The third category is called "*interdiction.*" Since each approach has various advantages and disadvantages, some cable systems use several methods in conjunction with each other to achieve various security goals.

Works Consulted

Jeff Adams, "HBO Continues Blazing New Paths" in ***TVRO Dealer***. July 1997, pp. 28-30, 32, 34, 74.

Thornton Howard Bridgewater and Doland G. Fink, "Television" in ***18 Encyclopedia Britannica*** Chicago, Illinois: Helen Hemingway Benton, 1974, pp. 105-23.

---------- "Cable: The First Forty Years" in ***Broadcasting.*** November 2, 1988, pp. 35-49.

John E. Cunningham, ***Cable Television.*** 2nd Edition. Indianapolis, Indiana: Howard W. Sams & Company, 1983, pp. 11-19.

Eagle Comtronics, Inc. "History of Cable Television Relating to Traps & Filters" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd, pp. 1-4.

General Instruments Corporation, ***CATV Reference Guide RD-16.*** Brownsville, Texas: GI Communications, 1995, passim.

General Instruments Corporation, ***Wiring Homes For Today's & Tommorrow's Cable Television Service.*** 1st Edition. Hickory, North Carolina: GI Corporation, nd, passim.

Magnavox CATV Systems, ***Cable TV Reference Guide***. Manlius, New York: North American Philips, 1991

William Grant, ***Cable Television.*** 1st edition. Reston, Virginia: Reston Publishing Company, Inc. 1983, pp. xiii - xx.

---------- "Man of the Year: Prince of the Global Village" in ***Time.*** January 6, 1992. pp. 20-39.

National Cable Television Association, ***Cable Television Developments: Industry Overview.*** Washington, D.C.: National Cable Television Association, 1994, *passim.*

National Cable Television Institute, ***Introduction to CATV.*** Denver, Colorado: National Cable Television Institute, Inc., 1983.

Scientific Atlanta, ***Broadband Communications Products***. Norcross Georgia: Scientific Atlanta, 1994.

Benjamin Estill Shackelford, "Television" in ***21 Encyclopedia Britannica.*** Chicago, Illinois: William Benton, 1946, pp. 909-13.

Archer S. Taylor, "Professor Crook: Inventor of CATV" in ***Communications Engineering Technology.*** June 1994. pp. 26-28.

Albert Warren, ***Television & Cable Factbook***. Washington, D.C.: Warren Publishing, 1997.

Chapter 2
Program Security

In 1992 the *National Cable Television Association* estimated that theft of basic and premium television services amounted to around $ 4.7-billion per year.[1] Compared with a total revenue of around $ 22-billion, the pay television industry may have lost more than twenty percent of its market to "piracy."

Satellite programming brought with it a proliferation of specialized entertainment intended to appeal to virtually every niche market conceivable. Nearly all satellite broadcasters charge cable operators a fee for carrying their channels. Fees are based upon the number of subscribers who receive the programming. Because *commercial satellite broadcasters,* like CNN, get most of their revenue from commercial advertising, the per subscriber fees charged operators for commercial programming is relatively low. Because *non-commercial satellite broadcasters,* like HBO, derive most of their revenue from cable operators, fees for non-commercial channels are higher.

With the introduction of satellite programming, operators needed a way of limiting the channels which subscribers receive to only those the subscribers were paying for. A variety of security methods have been developed since the middle 1970s to achieve that objective.

Program Security Methods

Program security methods may be divided into three broad categories - (1) cryptographic methods, (2) interdiction, and (3) passive filtering methods.

Cryptographic Methods

Virtually all cryptographic methods rely upon set-top converters to decipher programming. In general, these methods may be divided into two categories - (1) *analog methods,* and (2) *digital methods.* Analog methods are usually called "soft encryption" because they are easier to break than digital methods. Digital encryption methods are sometimes called "hard encryption" because they are believed to be more difficult to break. Analog methods may be divided into those which use *codes* and those which use *ciphers.*[2]

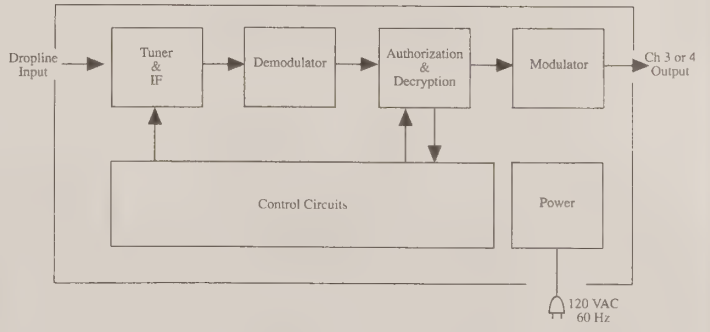
Analog Code Methods. Coding methods rely upon addressable set-top converters with unique serial numbers. Authorization codes for each set-top converter are imbedded in the video or in unused parts of the CATV spectrum. If the authorization code for a particular set-top converter is not received periodically, the set-top will automatically shut down. Two-way systems query the set-top converters in the system periodically. When an unauthorized serial number is detected, the headend computer sends a command to shut-down the unauthorized converter. More sophisticated systems transmit market codes and program tags with each program. Hence, specific tiers or pay channels may be authorized or deactivated from the headend.

[1] Norm Bedoucha, "Piracy on the High Seas of Cable" in ***Communications Technology.*** November 1995. p. 28.

[2]The terms "*code*" and "*cipher*" are frequently used incorrectly by those without any formal training in the field of *communications security.* All codes are ciphers but not all ciphers are codes. A "code" is defined as a system of signals used to transmit information. A code is a special form of substitution cipher. For example, a code symbol may be used to represent a letter, a word, a sentence, or an entire paragraph. Codes are frequently used merely to transmit information efficiently. E.g. Morse Code, ASCII, or "one if by land and two if by sea." A cipher involves a *cryptographic system* in which regular units of plain text are arbitrarily substituted or rearranged according to some per-determined "key" or algorithm. Where codes are "static " ciphers are dynamic.

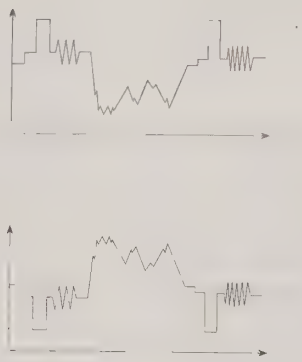
TYPICAL SET-TOP CONVERTER

Figure 2.1



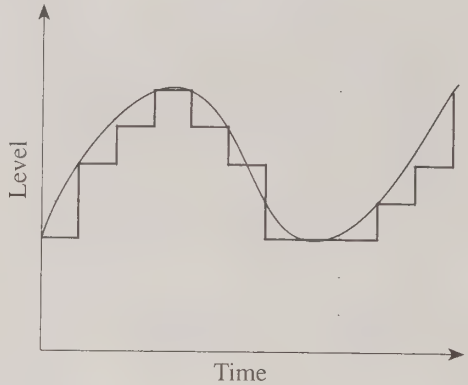
SAMPLE VIDEO INVERSION

Figure 2.2



A/D CONVERSION STEP WAVE

Figure 2.3



Analog Cipher Methods. Analog video ciphers simply *reformat* the television picture. Such ciphers rely upon methods like *video inversion, channel-inversion, sync-inversion, sync-suppression, gated sync-suppression, sync removal and replacement, sine-wave sync shifting, pulse sync-shifting, field inversion, line shuffle, line inversion, cut-and-invert, cut-and-rotate, or combinations of these methods.* Circuits for re-formatting the pictures are built into the set-top converter itself.

Such methods may be used to cipher either individual channels or entire groups of channels. They may also be used for *pay-per-view* (PPV) or "*impulse" pay per view* (IPPV) channels.

Digital Cipher Methods. Digital methods rely upon a two-step process for transforming analog video into a string of ciphered zeros and ones. Audio or video is *encoded* into digital information and then ciphered. The encoding of audio or video signals is called "analog-to-digital (A/D) conversion." Voltage levels are sampled at periodic intervals and "quantitized" into DC levels. This results in a "step-wave" which approximates the shape of the original analog signal. Each level in the step-wave is then represented by a digital code. Thus, this method of *coding* is called "*Pulse Code Modulation*" (PCM). The result is a stream of codes which represent the step-wave. This stream of digital codes is then "enciphered."

The higher the sampling frequency, the greater the quality of the reproduction. However, since each voltage level must be represented as a code, increasing the sample frequency also increases the speed requirements of the digital processors needed to encode or decode the signal.

There are a wide variety of digital encryption methods including *substitution*, *inversion*, *transposition*, *reversal*, *expansion*, *compression*, *blocking*, and *permutation*. Most digital encryption systems use several methods in conjunction with substitution.

Digital-substitution is the easiest method to understand. Using a *modulo two adder*, digital "plain text" may be bonded with a pseudo-random digital key string. A modulo two adder is simply an *Exclusive Or (XOR) Gate*. The pseudo-random key stream is just a string of meaningless zeros and ones which can be predictably generated using the "key." A pseudo-random "key stream" may be produced using a linear feedback shift register. A shift register is similar to a digital counter. When set to a particular setting, the register shifts zeros and ones from one stage to the next in a circular fashion. The original setting of the register can be modified in a particular pattern using various feed-back functions. With a simple n-bit shift register, the length of the key stream may be calculated by the number of "states" it can go through:

$$\mathbf{S = 2^n - 1}, \text{ where:}$$

S = number of states, and
n = the number of stages.

The number of states which a simple digital counter can go through is calculated as 2^n.

THE EXCLUSIVE OR (XOR) GATE
Truth Table

Table 2.1

Input A	Input B	Output C
0	0	0
0	1	1
1	0	1
1	1	0

The *decryption process* simply reverses the encryption process. Modulo-two adders have certain unique properties which make them ideal for digital encryption and decryption. *If plain text is added to a pseudo-random key stream using an XOR Gate, the result is a "ciphered text." However, if the key stream is added to the cipher text using the XOR Gate, the output will be the plain text.* The plain text may then be decoded using a digital-to-analog (D/A) converter. The result is a step-wave which approximates the original signal. The natural inductance and capacitance of the processing circuity will tend to "round" the edges of the step-wave resulting in a good approximation of the original program.

ENCRYPTION & DECRYPTION

Table 2.2

ENCRYPTION

Plain Text: 10110100
Key: ⊕ 11001100

Cipher Text: 01111000

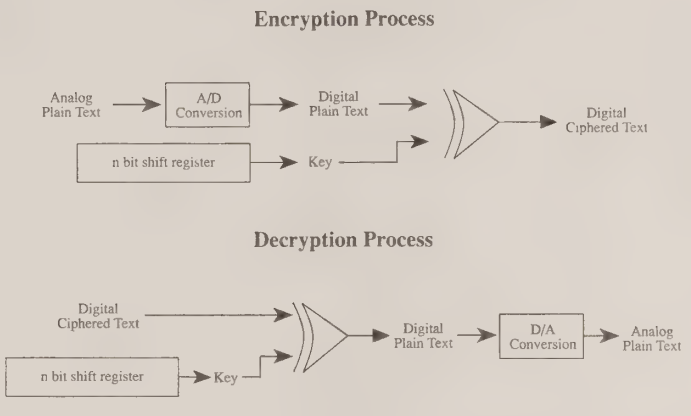
DECRYPTION

Cipher Text: 01111000
Key: ⊕ 11001100

Plain Text: 10110100

ENCRYPTION & DECRYPTION PROCESS

Figure 2.4

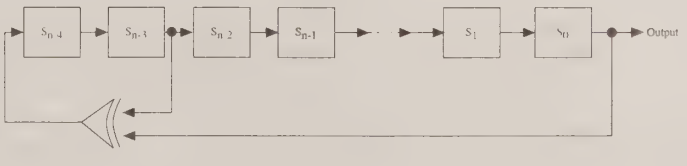


Digital Channel Compression. Digital channel compression is really a coding system used for fitting more than one program into a standard 6 MHz NTSC television channel. It relies upon a system of encoding (A/D conversion), reduction/compression, and multiplexing. By eliminating redundancies in a television picture it is possible to transmit the picture more efficiently. Once an initial picture is transmitted, only changes in the picture need be sent.

A digital multiplexer selectively looks at each of its data input lines sequentially. A set of data select lines determines which of the data inputs is selected as the output. A demultiplexer does exactly the reverse. Table 2.3 illustrates the digital inputs and outputs for the multiplexer illustrated in Figure 2.7. A digital key may be used to encipher each of the programs. Another digital master key may used to encipher the output. Hence, individual subscribers are given a special key which combines both keys for deciphering only the programs which they are authorized to receive.

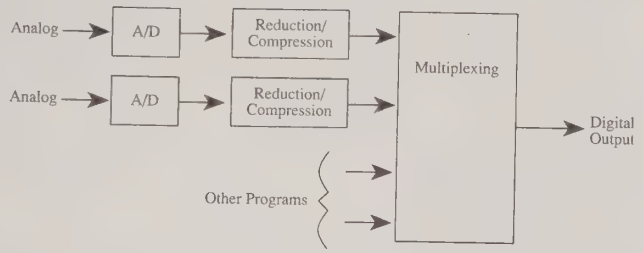
TYPICAL N-BIT SHIFT REGISTER

Figure 2.5



DIGITAL CHANNEL COMPRESSION

Figure 2.6



At the receiver, pictures are de-multiplexed, decompressed, and decoded using a D/A converter. Although digital compression technology itself may provide some security for a short period of time, any security it provides will be short lived as decompression circuitry becomes more common. *The basic encryption process remains no more secure than any other digital encryption system.*

Smart Cards. Some European cipher systems have introduced "smart card" technology. A smart card, containing sealed micro-processing circuits and memory chips, plugs into a set-top converter. Hence, the set-top's entire micro-processor may be changed periodically. Because smart cards are sealed, it is difficult for a pirate to examine the circuitry without destroying it. However, even if the algorithm is compromised, the operator may change the entire micro-processor in the subscribers' set-tops by simply distributing a new set of smart cards which will work with only specific set-tops.

DIGITAL MULTIPLEXING

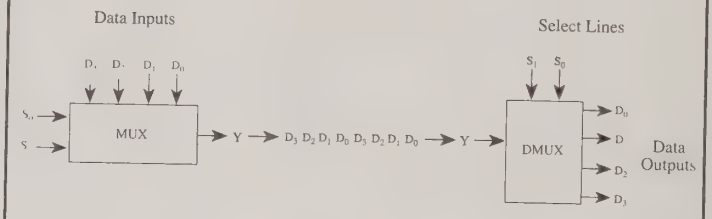
TRUTH TABLE

Table 2.3

Data Select		Data Inputs				Output
S_0	S_1	D_3	D_2	D_1	D_0	Y
0	0	0	0	0	1	1
0	1	0	0	1	0	1
1	0	0	1	0	0	1
1	1	1	0	0	0	1

MULTIPLEXING & DEMULTIPLEXING

Figure 2.7



Interdiction

When properly implemented, interdiction is probably one of the most secure, effective, and costly methods of protecting cable programming. It relies upon equipping each drop-line in the system with an "addressable tap."

Typical systems allow the operator to use between four and seven tiers. Each "tier" may be either a channel or a group of channels. Each tap may be addressed by the headend computer. A network of gated diodes, active filtering devices, and jamming carriers are used to block out channels or tiers which the subscriber is not authorized to receive. Interfering carriers - generated at the drop-line itself - are used to block aural and visual carriers on selected pay channels. By using frequency-hopping carriers, one oscillator can jam several different channels.

There are addressable taps which work like broadband "decoders" attached to the subscriber's drop-line. They may be used on any broadband cable system without equipping every tap in the system. However, such taps sometimes involve twice the expense of using a set-top converter plus the cost of installation.

Passive Filtering Methods

Passive filtering technology is one of the oldest and least expensive methods of securing programming. These techniques may be divided into two categories - (1) positive trapping, and (2) negative filtering.

Positive Trapping. Positive trapping methods rely upon "jamming" the television channel at the headend. A very narrow interfering carrier is inserted

between the aural and visual carriers in order to "jam the channel." The programming is recovered by placing a sharp trap or notch filter in the subscriber's drop-line. The trap "notches out" the interfering carrier with minimum damage to the program allowing the subscriber to view the interference free program. Thus, a trap is needed for *only those subscribers who are authorized to receive the premium channel.* Although positive trapping methods are less secure than negative trapping, many cable operators continue to use it because of its financial advantages.

Negative Filtering. Negative filtering methods rely upon placing a passive filter in the subscriber's drop-line to block channels which the subscriber is not authorized to receive. As long as the subscriber cannot remove the filter, negative filtering is very secure because the signals needed to assemble the television picture literally are not there. Thus, *a filter is needed for all subscribers who are not authorized to receive programming.*

Evaluating Program Security Systems

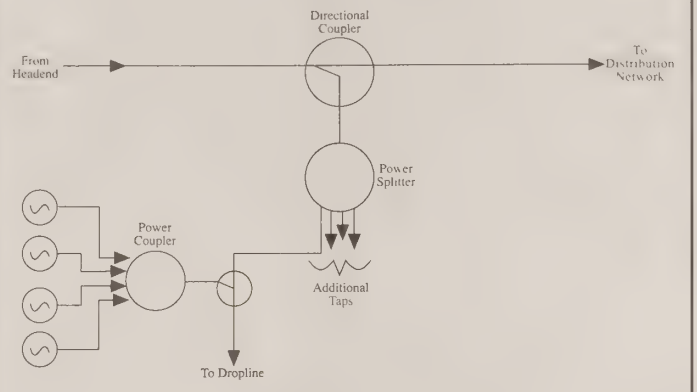
Despite large expenditures for research and development, none of the security systems developed by the pay television industry are *infallible.* Because each system has various advantages and disadvantages, it is not unusual to find operators using several systems to achieve various goals.

Cryptographic Systems. Set-top converters which use cryptographic systems have certain unique advantages. First, they allow operators to use a larger number of tiers and pay channels than is available using trapping methods. Second, set-tops allow operators to use PPV and IPPV channels. Third, tiers or pay channels may be authorized or de-authorized from the headend without a service call. This function is also useful when marketing pay channels since it is possible to authorized universal viewing during marketing campaigns. Finally encrypted signals are usually protected on trunk and feeder lines. Anyone connecting an unauthorized drop-line would still not receive a channel.

One of the chief disadvantages of cryptographic systems which rely upon set-top converters is that the converters are accessible to the customer.

ADDRESSABLE TAP
(Interdiction)

Figure 2.8



Consequently, they may be subject to examination, theft, or tampering. Systems which rely exclusively upon authorization codes may be defeated either by tampering with the circuity or by substituting a special pirate converter which cannot be shut down by the headend computer. Although stolen set-tops may be de-authorized from the headend, pirate set-tops are never *designed* to respond to headend commands.

When analog crypto systems were first introduced into satellite broadcasting during the mid-1980s they were touted as being "highly secure" because of the vast number of possible keys. Today, most of those systems have been broken by "hackers."[3]

Typically the designers of new ciphers point out how long it would take a computer to run through all possible combinations of a system's keys. However, it should be understood that the number of possible keys a cryptographic system has *does not necessarily measure the security of the system.* Few cryptanalysts rely upon "brute force attacks" which involve trying every possible key. Cryptanalysts look for weaknesses in the system and then exploit those weaknesses. Further, increasingly sophisticated computer technology is making more computational power available to the average viewer every day.[4]

[3]A significant number of analog ciphers were actually broken by hackers the same day they were introduced. For specific details cf. Frank Baylin, John McCormic, & Richard Maddox, ***World Satellite TV & Scrambling Methods***; Brent Gale & Frank Baylin, ***Satellite & Cable TV Scrambling & Descrambling***; and John McCormic, ***European Scrambling Systems.***

Most video technicians can quickly determine how an analog video cipher works by simply looking at the video with an oscilloscope. It is even possible to build the circuits needed to re-format the video without ever seeing the set-top converter. For example, most sync-displacement ciphers can be defeated by clipping all of the sync pulses and reinserting them in their proper places. Video inversion ciphers are defeated by simply re-inverting the video.

Cipher systems are extremely fragile. Theoretically, if both the ciphered text and the plain text which it conceals are compromised, *the cipher can be quickly broken.*

In military systems *both* the key and the "secret" plain text messages are carefully protected against compromise. Used keys and messages are scrupulously shredded and burned. Keys are distributed in advance by the *Armed Forces Courier Service* and changed daily. Cipher systems are carefully designed so that the key used in any given communications link is unique. Yet even very sophisticated digital ciphers have been broken.[5]

The pay-television industry faces a very perplexing theoretical problem. *Because the "plain text" of premium video channels is "public" and usually widely available, a truly secure program cipher is theoretically impossible.* Hence, *no matter how sophisticated or expensive* a program security system may be, if a hacker can obtain a copy of both the *plain text* and the *ciphered text*, it is possible to quickly *deduce the key stream.* This, of course, is easier to do *if one already has access to the de-cryption equipment.*

Deduction of a digital key-stream allows one to determine how the key-stream was generated. Compromise of a key is catastrophic because once the cryptanalyst has the key she or he can read all of the communications which have been enciphered using it. Further, *once ciphered program signals are inside a subscriber's residence, it is virtually impossible to "police" those signals or what the subscriber does with them.*[6] Since practical program security systems must rely upon either *pre-programmed keys* or *keys sent over the communications-link itself,* such systems are very vulnerable to analysis.[7]

In military systems, *sending a cipher key over a communications link is a mortal sin.* Although smart cards avoid the security compromises involved in sending keys over the cable, they are costly. Programming 20,000 smart cards and sending them to subscribers sometimes represents a logistical nightmare.

The danger to cipher-systems is not that thousands of subscribers will turn into amateur cryptoanalysts and build their own code breaking equipment. *The danger is that a few hackers will either sell inexpensive "black boxes" or sell black box plans which are capable of defeating systems worth millions of dollars.*[8]

While it is possible to design more complex cipher systems which are more difficult to "hack," increased complexity involves increased cost, more complex

[4]Actually, modern computer technology is an outgrowth of technology originally developed for war-time code breaking. Virtually all contemporary personal computers have far more computational power than the "computers" used to break the famous German *Enigma* cipher. The Enigma cipher had 159 x 10^{18} possible daily keys. Cf. F.H. Hinsley and Alan Stipp, eds., ***Code Breakers: The Inside Story of Bletchley Park.*** p. 86.

[5]As a result of disclosures in the "Walker family spy case," it is believed that the Soviet Union may have broken the digital cipher associated with the TSEC/KW-7 during the late 1960s or 1970s. The KW-7 was one of several crypto devices hijacked by the North Koreans aboard the U.S.S. Pueblo on January 23, 1968.

[6]It is legally arguable that the subscribers who decipher programming with their own equipment have not committed any crime since they are merely "re-formatting" signals supplied by the cable operator.

[7] "Woe is he who arrogantly believes that his cipher is unbreakable." We now know that de-cryption of German and Japanese messages may have given the allies a decisive advantage in winning the Second World War. Until 1973 much of this secret history was kept under wraps.

[8]Chapter 8 will illustrate the reality of this danger. Between 1989 and 1995 authorities confiscated more than a half million pirate "decoders" and pirate set-top converters. Cf. Dy Rheu Kuston, Henry Schwah, and Susphun Paggan, "Combating Cable Signal Theft" in ***CED***. June 1995. p. 60.

DEDUCING A DIGITAL KEY

Table 2.4

ENCRYPTION

Plain Text:		10110100
Key:	⊕	11001100

Cipher Text:		01111000

DECRYPTION

Cipher Text:		01111000
Key:	⊕	11001100

Plain Text:		10110100

KEY DEDUCTION

Cipher Text:		01111000
Plain Text:	⊕	10110100

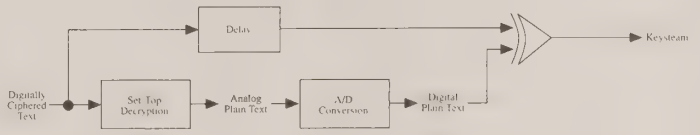
Key:		11001100

maintenance, and increased financial risk. Although digital systems are believed to be "far more secure" than analog systems, the fundamental theoretical problem remains. If both the cipher text and plain text are available, it is possible to deduce the cipher key used to encrypt the plain text. *Cipher systems simply don't work when the plain text is made public.*

Because most television sets are now cable compatible, set-top converters are no longer required for converting channels. When required solely for security purposes, they interfere with features on the subscriber's television or VCR. Set-top converters also complicate the installation of additional outlets in the subscriber's home since a separate converter is needed for each television set. This inflates the cost of multi-set installations.[9] For these reasons, customers tend to dislike them. Because set-top converters are in customers' homes, they may be subject to abuse. Since set-top converters are complex devices, repair and maintenance is more complex and costly than devices which have no active components.

A METHOD FOR ANALYZING DIGITAL CIPHERS

Figure 2.9



Interdiction. When properly implemented, interdiction using addressable taps is probably one of the most effective methods yet devised. Because services can be activated or deactivated remotely, service calls to modify service are unnecessary. Thus, services like PPV and IPPV can be easily implemented. It is also possible to authorize universal viewing of pay channels during marketing campaigns. Since addressable taps are outside the customer's home, they are less likely to be abused or damaged. However, for several reasons, interdiction is *extremely expensive.*

Inexpensive interdiction systems which use "pure-frequency carriers" or carriers which hop at regular rates can be defeated. This can be done by frequency-cancellation using an inverted carrier with an identical frequency keyed at exactly the same rate. Interference carriers should hop at pseudo-random rates with variable off-sets and be modulated using a pseudo-random signal. Of course, this drives up the cost of the interdiction equipment.

Interdiction is also expensive because every drop-line must be equipped with an addressable tap in advance even if the drop-line is for a non-subscribing household. Another factor which inflates costs is that both basic customers and premium customers require addressable taps. Even if only subscriber taps are equipped with addressable taps, the cost of each unit is more than the cost of a set-top converter plus installation expenses. Because addressable taps are

[9]The flip side of this is that it is not possible to pirate service from one apartment to another using an additional outlet connected to a subscriber's drop-line without a set-top converter.

complex devices, maintenance is more complex and costly than passive equipment. Finally, unlike set-top converters which run on the subscriber's power, each tap uses power purchased by the cable operator even if it is on a non-subscribing drop-line. Thus, monthly power costs are much higher. Unlike cryptographic systems, premium channels protected using interdiction are "clear" on trunk and feeder lines. Hence, anyone connecting an unauthorized drop will receive the service if they bypass the tap.

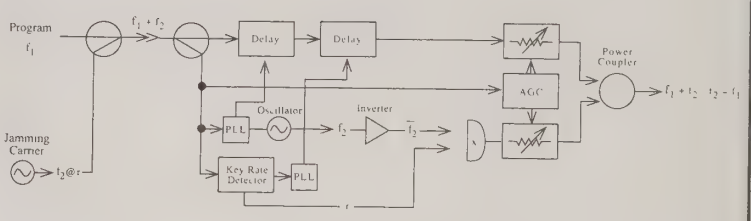
Positive Trapping. Positive trapping methods have a variety of disadvantages. First, PPV and IPPV services are not available using positive traps. Second, the number of channels which can be protected is usually limited by the amount of insertion loss which can be tolerated in the drop-line. Third, a service call is necessary to activate or deactivate service. Fourth, positive trapping is usually easy to defeat. If a pirate can either make, purchase, or steal an appropriate filter, the premium service can be easily recovered. Obviously, there is no way of detecting whether a basic customer is doing this. Yet, despite its disadvantages, the low cost of positive trapping makes it a very attractive security option.

A number of companies have "beefed up" the positive security system with a variety of innovations which make it more difficult to fabricate "pirate filters." Because pay channels are jammed at the headend, it is possible for the cable operator to turn off the jamming carrier in order to allow all customers to view a pay service for a limited period of time. This makes it easy for cable operators to run sign-up campaigns which give viewers a "taste" of a premium pay channel. Like interdiction, positive trapping simplifies the installation of additional outlets. However, unlike addressable taps and set-top converters, positive traps are *simple passive devices*. Maintenance is virtually nil and replacement is easy and straightforward. Like cryptographic systems, channels which are jammed using a positive security system are jammed on trunk and feeder lines. Thus, anyone connecting an unauthorized drop-line will still not receive the service.

When negative traps are used, the operator must supply a trap for every customer who is *not* authorized to receive premium channels. Thus, if a system has 20,000 subscribers with 5,000 premium

DEVICE FOR DEFEATING SIMPLE INTERDICTION

Figure 2.10



subscribers, the operator must purchase 15,000 traps. With positive trapping methods, the operator need only buy traps for customers who are authorized to receive premium channels. Hence, in the previous example, the operator would only have to buy 5,000 traps for the premium customers.

Negative Filtering. Like positive trapping methods, the number of negative filters which can be used on a drop is limited by the amount of insertion loss which the drop-line can tolerate. As with positive trapping, *PPV* and *IPPV* services are not available using negative filters. A service call is necessary to connect, disconnect, or modify services. Like systems which use interdiction, premium channels are "clear" on trunk lines and feeder lines. Thus, anyone tapping into the lines to connect an unauthorized drop-line will receive the service. However, negative filters have a variety of significant advantages.

As with interdiction and positive trapping, the installation of additional outlets is easy and inexpensive. Negative filters do not interfere with features on the subscriber's television or VCR. Further, negative filtering methods are *one of the most secure methods of controlling programming*. They literally prevent essential program signals from entering the subscriber's residence. Without these signals, the subscriber's television cannot assemble an intelligible picture. Like positive traps, negative filters are maintenance free passive devices which are easily replaced.

Although it is possible to remove negative filters from the tap, a pirate *must commit the crimes of*

PROGRAM SECURITY METHODS

Advantages & Disadvantages

Table 2.5

Type	Advantages	Disadvantages
Converters	Less expensive than interdiction Optional PPV or IPPV More tiers available Change services without service call Universal authorization for marketing Can usually be used with traps Signal protected on trunk and feeder lines	More expensive than traps Can be defeated or circumvented Compromise usually not detectable Interferes with TV & VCR features Complicates additional outlets Use with multiple TVs costly for customer Customers dislike them Complex maintenance
Interdiction	Relatively secure Optional PPV or IPPV Change service without service call Universal authorization possible for marketing Additional outlets easy to install Does not interfere with TV or VCR	Most expensive Compromise may not be detectable Complex maintenance Signals not protected on trunk and feeder lines Usually requires equipping all taps
Positive Traps	Frequently least expensive option Universal authorization for marketing possible Additional outlets easy to install Does not interfere with TV or VCR Can be used with set-tops Highly reliable Inexpensive maintenance Signals protected on trunk and feeder lines	Sometimes relatively easy to defeat with stolen, purchased, or fabricated traps Compromise not detectable No PPV or IPPV Limited tiers Service call necessary to change service
Negative Filters	Relatively secure Relatively inexpensive Requires legal infraction to defeat Compromise detectable Additional outlets easy to install Does not interfere with TV or VCR Can be used with set-tops Highly reliable Inexpensive maintenance	Limited tiers No PPV or IPPV Service call necessary to change service Signals not protected on trunk and feeder lines

trespass, vandalism, and theft of services in order to defeat a negative filter. Further, the compromise is *detectable* through periodic audits. Although negative filtering methods are usually more expensive than positive trapping methods, use of negative filters is far less expensive than set-top converters or interdiction. Where a set-top converter costs between $ 50.00 and $ 300.00 - depending upon its complexity - filters range between $ 5.00 and $ 20.00 each depending upon the quantity ordered. For these reasons, many systems continue to use a combination of negative traps and set-top converters.

Works Consulted

Mike Bates and Robert Depweg, "How Continental of LA Thwarted Complex Piracy Ring" in ***Communications & Engineering Design.*** June 1994. pp. 58, 62, 60, 64.

Frank Baylin, John McCormic, and Richard Maddox, ***World Satellite TV and Scrambling Methods: The Technicians Handbook.*** 3rd Edition. Boulder, Colorado: Baylin Publications, 1993.

Henry Becker and Fred Piper, ***Cipher Systems: The Protection of Communications.*** New York: John Wiley and Sons, 1982.

Norbert Bedoucha, "Piracy on the High Seas of Cable" in ***Communications Technology.*** November 1995. pp. 28, 30.

Bruce Bosworth, ***Codes, Ciphers, and Computers: An Introduction to Information Security.*** Hasbrouck Heights, New Jersey: Hayden Book Company, Inc., 1982.

Roger Brown, "Whole-House Service Gets A Face Lift" in ***Communications Engineering & Design***. June 1997. pp. 68, 70, 77.

Eagle Comtronics, Inc., "Application Notes: Sideband Interdiction System EE-3000" [Technical Monogram; AN903002 Rev. 0]. Clay, New York: Eagle Comtronics, Inc., 1995.

James O. Farmer, "Subscriber-Ready Cable?" in ***Communications Technology.*** May 1993. pp. 30-32, 34, 36, 52-54.

Thomas L. Floyd, ***Digital Fundamentals.*** 4th Edition. Columbus, Ohio: Merrill Publishing Company, 1990.

Helen Fouche Gaines, ***Cryptanalysis: A Study of Ciphers and Their Solution.*** New York, N.Y.: Dover Publications, 1939.

Brent Gale and Frank Baylin, ***Satellite and Cable TV Scrambling and Descrambling.*** 2nd Edition. Boulder, Colorado: Baylin/Gale Publications, 1986.

Norma Gleason, ***Cryptograms and Spygrams.*** New York, N.Y.: Dover Publications, 1981.

Paul A. Harr, "Movies on Demand: the Next Step for PPV" in ***Communications Technology.*** May 1993. pp. 24, 26, 50.

F.H. Hinsley and Alan Stipp, eds., ***Code Breakers: The Inside Story of Bletchley Park.*** Oxford, England: Oxford University Press, 1993.

Stephen Holmes, "Cable TV Data Network Security System: Thwarting Hacking & Fraud" in ***Communications Engineering Technology.*** December 1994. pp.60, 62, 64,

David Kahn, ***The Codebreakers: The Story of Secret Writing.*** New York, N.Y.: Macmillan Company, 1967.

David Kahn, ***Seizing The Enigma: The Race To Break The German U-Boat Codes, 1939-1945.*** Houghton Mifflin, 1991.

Dy Rheu Kuston, Henry Schwoh, and Susphun Pagann, "Combatting Cable Signal Theft" in ***Communications & Engineering Design.*** June 1995. pp. 58, 60 - 63.

William A. Krepick, "Keeping PPV Under Lock & Key" in ***Private Cable & Wireless Cable***. April 1995, pp. 17, 18.

John Lamrande, "Building A Better Mousetrap" in ***Communications & Engineering Design.*** *June 1993. pp. 72, 74, 77.*

Lawrence W. Lockwood, "Cryptography for Video Security" in ***Communications Technology.*** March 1995. pp. 24, 26, 28, 32.

Lawrence W. Lockwood, "A/D and D/A" in ***Communications Technology.*** December 1994. pp. 26, 28, 30, 32, 34.

Henry Lysing, ***Secret Writing: An Introduction to Cryptograms, Codes, and Ciphers.*** New York, N.Y.: Dover Publications, 1974.

John McCormac, ***European Scrambling Systems: Circuits, Tactics, and Techniques.*** Waterford, Ireland: Waterford University Press, 1993.

National Cable Television Association, ***Signal Security Handbook: A Resource Manual for Cable Operators.*** Washington , D.C.: National Cable Television Association, 1993.

National Cable Television Association and the Coalition to Oppose Signal Theft, "Cable Theft Is A Crime: Education Kit [Loose Leaf Folder]. Washington, D.C.: National Cable Television Association, nd.

Mitchell Olfman, "Developments in Addressable Control and Signal Security" in ***Communications Technology.*** June 1994. pp. 90, 92, 94, 146,

Paul Paradise, "Signal Theft" in ***Electronics Now.*** January, 1995. pp. 33-40, 90.

Pico Products, Inc., "Collected Filter Specifications & Spectrum Plots" [Loose leaf collection of photocopied spectrum plots and product information provided by manufacturers representative]. Liverpool, New York: Pico Products, Inc., nd [1994].

Norman Polmar and Thomas B. Allen, ***Spybook: The Encyclopedia of Espionage.*** New York: Random House, 1977.

Robert J. Rance, "Tips On Network Security" in Communications Technology. May 1997, pp. 50, 51

Bill Rivas, "Jones Intercable's Theft of Cable Amnesty Program" in ***Communications & Engineering Design.*** June 1996. pp. 94, 96, 98, 99.

Ronald Schaffner, "The Trade Off" in ***Wireless International.*** July 1991. pp. 26-28, 31.

Kathleen Scoop, Barry Rosenblum, and Daniel J. Lefkowitz, "Time-Warner Cable NYC Attacks Theft At All Levels" in ***Communications & Engineering Design.*** June 1996. pp. 100, 102, 104.

Lawrence Dwight Smith, ***Cryptography: the Science of Secret Writing.*** New York, N.Y.: Dover Publications, 1971.

Bill Spies, "Impulse Pay Per View: Is Today's Much Different (or better) Than Yesterday's?" in ***Communications Technology.*** May 1993. pp. 20, 21, 44, 45, 46, 47.

Graham Stubbs, "Conditional Access Via Digital Decompression" in ***Communications Technology.*** March 1993. pp. 32, 50, 51.

---------- ***Understanding Computers: Computer Security.*** Alexandria, Virginia: Time-Life Books, 1986.

Tony Wasilewski, "The Benefits of Public Key Cryptography" in ***Communications Engineering & Design.*** May 1996. pp. 95-98.

Anthony J. Wasilewsky, "Public Key Cryptography in Broadband Nets: Part 1" in ***Communications Technology.*** December 1996. pp. 70, 72, 76, 78, 80.

Anthony J. Wasilewsky, "Public Key Cryptography in Broadband Nets: Part 2" in ***Communications Technology.*** January 1997. pp. 52, 54, 56.

Peter Way, ***Codes and Ciphers.*** New York, N.Y.: Dover Publications, 1977.

Tony Wechselberger and George Parkanyi, "Methodologies for Conditional Access Technologies in Digital Delivery Systems" in ***Communications Technology.*** June 1194. pp. 74, 78, 80, 82, 84, 86, 88.

Chapter 3
History of Pay Television Filtering

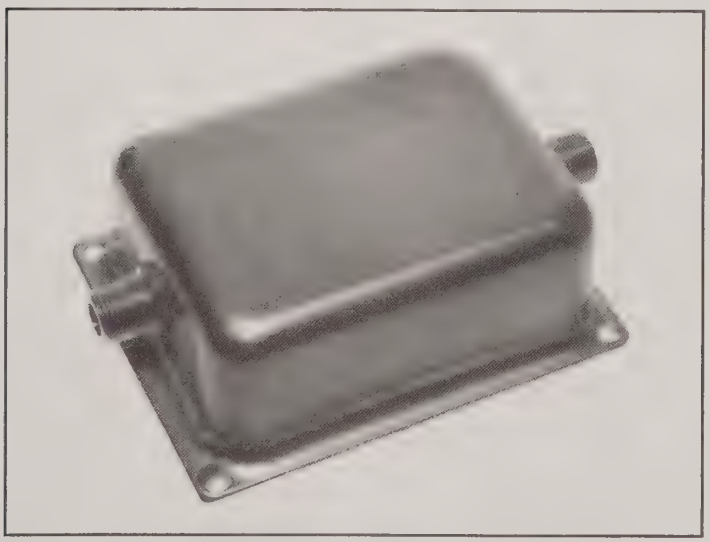
The introduction of premium channels created a need to limit reception to only those subscribers who were authorized to receive them. The first pay television filters were negative traps intended to block reception of premium channels. Initially the subscriber's own television limited reception to the VHF lowband (Channels 2 -6), the VHF highband (Channels 7-13), and the UHF band. Since VHF mid-band channels are placed between Channels 6 and 7, it was possible for an operator to use a set-top converter for supplying premium service. Although this strategy could be circumvented by people with some technical knowledge, during the early days of cable it worked in many small systems. As previously noted, this security strategy became completely ineffective when *generic* set-top converters hit the market. Hence, operators had to resort to more secure filtering methods to limit reception. Although technology has become more sophisticated over the years, the basic outlines of the "cable pirate war" have not changed.

History

The term "trap" is actually a *non-technical slang term.* It first appeared in *amateur radio literature* to describe either a series-resonant circuit used in an antenna for shorting problem frequencies to ground or a parallel resonant circuit used for making a multi-band antenna. *We use the term to refer to a narrow bandstop filter or "notch."* However, some cable installers refer to "traps" as *any* cylindrical filter regardless of whether the filter is a low pass filter (LPF), highpass filter (HPF), bandpass filter (BPF), or bandstop filter (BSF). *We reject this usage* because it is so broad as to mean little more than "cylindrical filter." Nevertheless, occasionally we use the term in the most general sense. Early cable operators adopted the term because they learned how to make simple notch filters from amateur radio operators.

The first pay TV traps were homemade devices constructed with coiled coaxial cables. The inner conductor of a coaxial cable was shorted to the shield at a specific interval in order to tune the notch to a specific channel. The coiled cable was then held together using tie-wraps. Because the notches were wide, three channels were required in order to trap out a single premium channel. However, since cable systems had a lot of spare spectrum, this disadvantage was not too serious. Later traps made by *Vitek* were coaxial cables with a twin center load. One conductor was modified to be a parallel resonant circuit.

As more premium channels became available spectrum space became more limited. A need arose for narrower traps with wider passbands. Operators could no longer afford to sacrifice two channels for each premium channel they carried. Eventually



Some of the first pay traps were made in "blister cans" which were connected to taps using a coaxial jumper (Photo by C & E Corp)

In the 1970s Marty Zelenz developed an improved trap enclosure similar to that shown (Photo by C & E Corp.)

coiled cable traps were replaced with filters made using discrete components. Discrete components allowed designers to make traps with much narrower stopbands. The new filters also had wider passbands allowing the operator to use higher channels. Inductors and capacitors were mounted on a printed circuit board inside a rectangular metal can with male and female "Type F" connectors at each end. Sometimes these traps were handmade.

The first pay television traps had some problems. Eventually customers learned how cable operators were limiting their reception. A customer could climb a pole and open the can using vice grips in order to retune the trap to receive premium service. Since the traps were in bulky cans, they had to be connected to the taps using jumper cables. The additional connectors increased the insertion loss of the trap and introduced additional problems associated with connector corrosion. Because the traps rusted easily, they had to be replaced periodically.

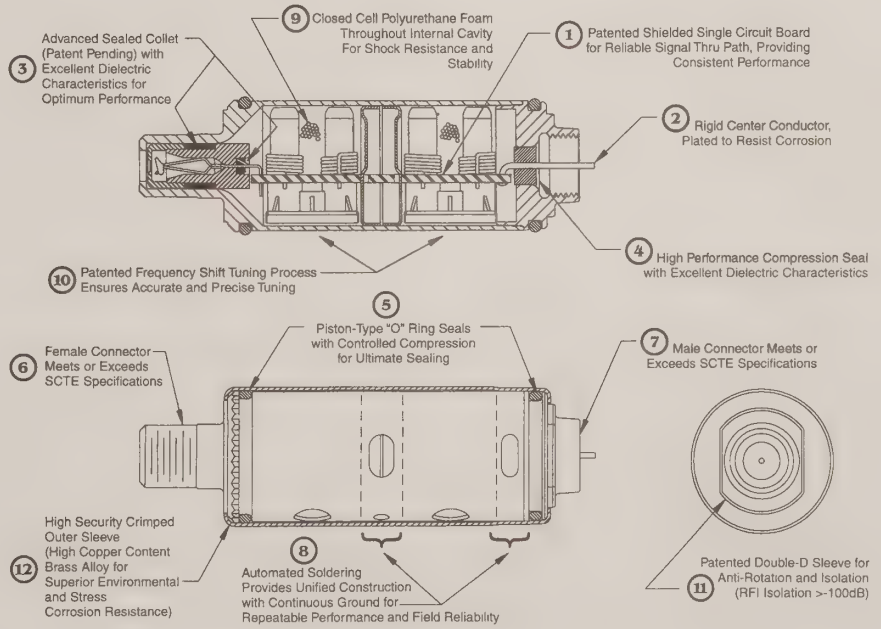
As larger cable systems began to spring up in metropolitan areas, operators needed less expensive traps in much larger quantities. Mass production techniques were introduced to make lower cost traps in large quantities. With a need for relatively simple filters in large quantities, numerous filter manufacturers rushed their own unique traps to market. Nevertheless, there was a real need for low cost traps which were compact, weatherproof, mechanically rugged, and resistant to vandalism.

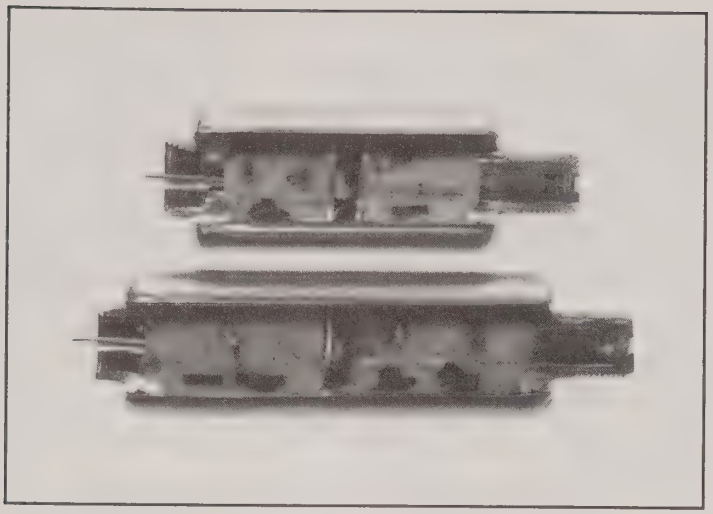
During the 1970s, Marty Zelenz developed a more rugged trap enclosure. In fact, Zelenz's basic design is still used today. Zelenz placed a narrow rectangular circuit board inside a double metal cylinder with Type F connectors mounted at each end.[1] The cylinder was 0.812-inches in diameter. This allowed cable installers to connect the traps directly to the tap without using any jumpers. Because of their design, double cylinder traps were very difficult to break open. Two internal

[1]*Eagle Comtronics* was originally founded in the early 1970s to produce cylindrical pay television filters by Alan Devendorf, Jarvis Fletcher, Ken Kennedy, Andy Tresness, and Marty Zelenz. Originally, Andy Tresness sold *Eagle's* first contract, provided financing, and served as President and Chairman of the Board. When demand exceeded *Eagle's* resources, *Eagle* entered into a joint venture with *Pico Products* (*Eagle's* subcontractor for printed circuit boards) to produce the filters. Bernard Hitchcock of *Pico* first applied *volume manufacturing techniques* to produce the filters for *Eagle*. Eventually Fletcher, Kennedy, Tresness, and Zelenz left *Eagle*. Tresness later *founded Arcom Laboratories* to compete with *Eagle* and *Pico* which had terminated their joint venture.

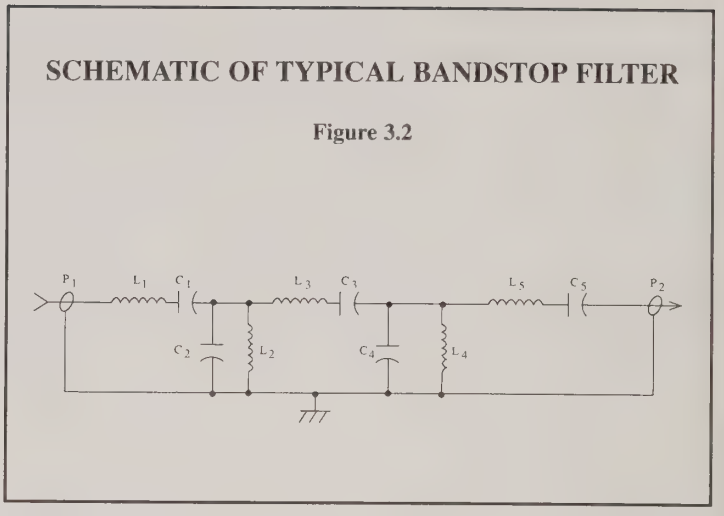
MECHANICAL DRAWING OF PAY-TV FILTER
(Courtesy of Eagle Comtronics)

Figure 3.1


9 Closed Cell Polyurethane Foam Throughout Internal Cavity For Shock Resistance and Stability
1 Patented Shielded Single Circuit Board for Reliable Signal Thru Path, Providing Consistent Performance
Advanced Sealed Collet (Patent Pending) with 3 Excellent Dielectric Characteristics for Optimum Performance
2 Rigid Center Conductor, Plated to Resist Corrosion
4 High Performance Compression Seal with Excellent Dielectric Characteristics
10 Patented Frequency Shift Tuning Process Ensures Accurate and Precise Tuning
5 Piston-Type "O" Ring Seals with Controlled Compression for Ultimate Sealing
6 Female Connector Meets or Exceeds SCTE Specifications
7 Male Connector Meets or Exceeds SCTE Specifications
High Security Crimped Outer Sleeve (High Copper Content 12 Brass Alloy for Superior Environmental and Stress Corrosion Resistance)
8 Automated Soldering Provides Unified Construction with Continuous Ground for Repeatable Performance and Field Reliability
Patented Double-D Sleeve for 11 Anti-Rotation and Isolation (RFI Isolation >-100dB)



Cut-away of Arcom pay television filters. (Photo by C & E Corp.)



compression rings were used as weather seals. This prevented moisture from getting into the trap. The compact cylindrical design made it easy to connect several traps to the same tap.

Until 1978 all pay television filters were "negative traps" which stopped signals from entering the subscriber's home. But in 1978 James L. Tanner patented a new pay television system.[2] The system was called the "TEST Positive Security System" after Tanner's company - *Tanner Electronic Systems.*

Tanner called it a "positive" security system because it relied upon an "active" signal to jam television pictures rather than purely passive filtering devices. The system worked by inserting a narrow interfering carrier into the television channel at the cable headend in order to "jam" or interfere with the program. A narrow notch filter was then used at the subscriber's tap to filter out the jamming carrier. Although most cable operators and filter manufacturers refer to these processes as "coding" and "decoding," cryptographers would call the Tanner approach a "jamming" system.

Design

Eventually, the construction, packaging, and performance requirements for pay television traps became standardized. The filters were invariably designed in a "ladder network." Four pole filters are usually sufficient for single channel traps. Tiering traps have up to sixteen poles.

Construction. Because filters are frequently mounted in elevated locations for security purposes, they must be shock resistant. If an installer drops a filter from a twenty-foot utility pole it must not de-tune. Since people have been known to tamper with filters in order to pirate free premium service, filters must be resistant to vandalism.

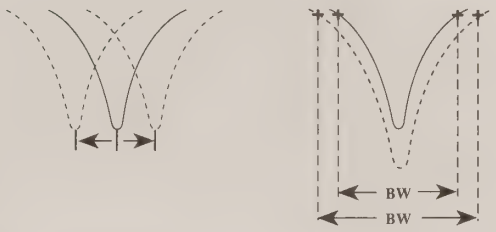
Weatherproofing. Because pay filters are mounted outside, they must be completely weather sealed. Moisture in a filter will cause corrosion. Moisture can also have a more immediate impact. It can cause the dielectric constant of a coil or capacitor to change. If the dielectric constant varies, the value of the component will change. This will cause the filter to change frequency or *drift* as the humidity changes.

Temperature Stability. Because pay filters are mounted outside, temperature stability is important. When temperature changes, most material either expands or contracts. Such changes can alter component values causing filters to change frequency. If notches change frequency with changes in temperature, they may end up blocking the wrong channel while passing premium service to unauthorized customers. Thus, filters must be "temperature compensated" so they don't drift. This is done by carefully selecting capacitors with temperature characteristic which are opposite to those of the coils selected for the filter. When one value increases with temperature another component value

[2]The original Patent for the "TEST Positive Security system" was issued on February 14, 1978 as Patent No. 4,074,311.

REDUCING TEMPERATURE SENSITIVITY OF A FILTER

Figure 3.3



decreases. Thus, opposite variations tend to neutralize each other.

Another method of reducing the temperature sensitivity of notches is to widen their stopbands. This can be done by simply deepening the notch. However, if the notch is too wide it will attenuate the adjacent channel carriers. Thus, there is a trade-off between notch depth and adjacent channel loss.

Many filter manufacturers have environmental test chambers which allow them to test filters over a specified period of time. The temperature inside the chamber can be programmed to vary over a specified period in order to monitor filter performance under various temperature conditions.

Leakage Requirements. Pay television traps must be electrically sealed. Cable signals should not leak out of the trap and outside signals should not leak into the trap. If signals leak into a trap they may enter the subscriber's drop-line and create interference. Worse still, they may leak into the cable system and cause problems for everyone connected to the system. If cable signals leak out they could interfere with broadcast television channels or even air navigation frequencies. Since some of the frequencies used on cable systems are also used for air navigation, the FCC has established stringent leakage requirements for cable television systems.

Some pay filter manufacturers have leakage test chambers for testing the amount of signal which leaks out of the filter. A chamber is necessary because it is possible for stray radio frequency fields to be confused with fields emanating from the filter. Usually filters are tested at much higher power levels than those used on the drop-line. For example, *Pico Products Inc.* tests their filters using a power level equal to 0.5 watts.

FCC Leakage Requirements (47 CFR 76.607)

Table 3.1

Frequencies (MHz)	Leakage Limit (µV/m)	Distance (meters)
Less than 54 and over 216	15	30
Over 54 up to and incl. 216	20	3

For operation in the frequency bands 108 - 137 MHz and 225 - 400 MHz, refer to paragraph 76.610.

Channel	Frequency (MHz)	20 µV/m	50 µv/m
2	55.25	- 35.3 dBmV	- 27.3 dBmV
4	67.25	- 37.0 dBmV	- 29.0 dBmV
6	63.25	- 38.8 dBmV	- 30.9 dBmV
FM	90.00	- 39.5 dBmV	- 31.5 dBmV
FM	95.00	- 40.0 dBmV	- 32.0 dBmV
FM	100.00	- 40.4 dBmV	- 32.5 dBmV
FM	105.00	- 40.8 dBmV	- 32.9 dBmV
60	109.25	- 41.2 dBmV	- 33.2 dBmV
14	121.25	- 42.1 dBmV	- 32.9 dBmV
16	133.25	- 42.9 dBmV	- 33.2 dBmV
19	151.25	- 44.0 dBmV	- 34.1 dBmV
7	175.25	- 45.3 dBmV	- 35.0 dBmV
10	193.25	- 46.1 dBmV	- 36.1 dBmV
13	211.25	- 46.9 dBmV	- 37.3 dBmV
27	241.25	- 48.1 dBmV	- 40.1 dBmV
32	271.25	- 49.1 dBmV	- 41.1 dBmV
37	301.25	- 50.0 dBmV	- 42.0 dBmV
42	331.25	- 50.6 dBmV	- 42.9 dBmV
47	361.25	- 51.6 dBmV	- 43.6 dBmV
52	391.25	- 52.3 dBmV	- 44.3 dBmV

$$V\ (dBmV) = 20 \log_{10} [\ E(\mu\ V/m) / (\ 0.021 * f\ (MHz)\ )\ ] / 1000$$

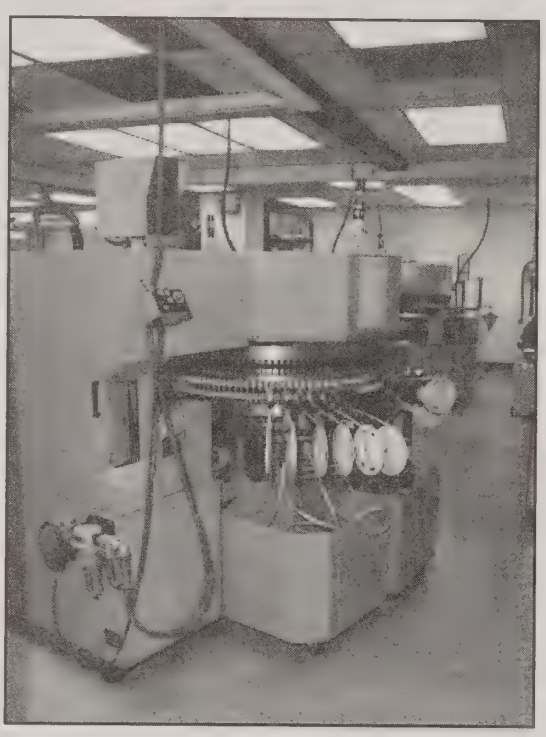
Note: Correct as appropriate for antenna gain, preamp gain, cable loss, and distance between cable and antenna greater than 3.0 meters

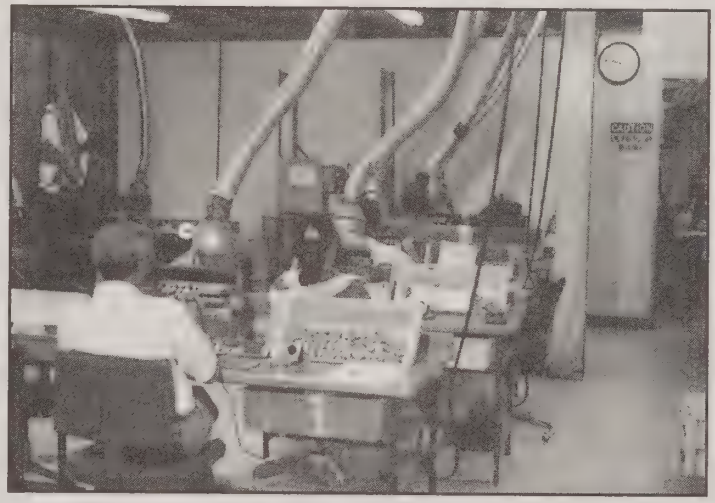
Production

Modern pay television filters are mass produced. Bernard Hitchcock first applied volume manufacturing techniques to the production of cylindrical pay television filters. Circuit boards are

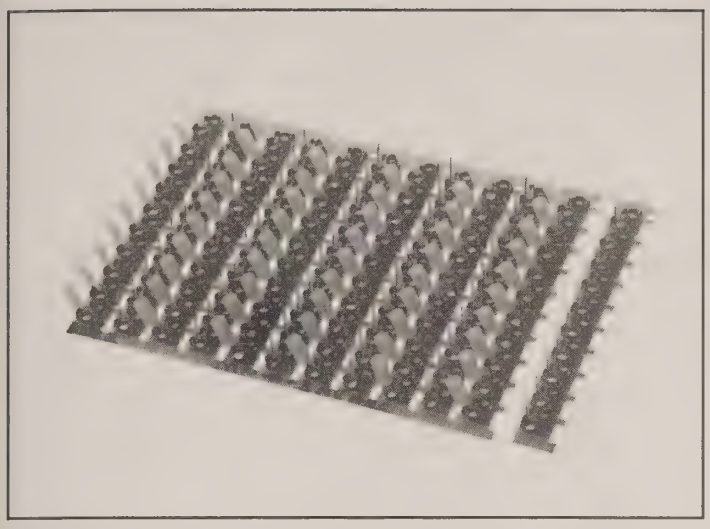
VOLUME MANUFACTURING TECHNIQUES

(Photos from Arcom Laboratories by C&E Corp.)





Bernard Hitchcock first applied volume manufacturing techniques to pay television filter production.



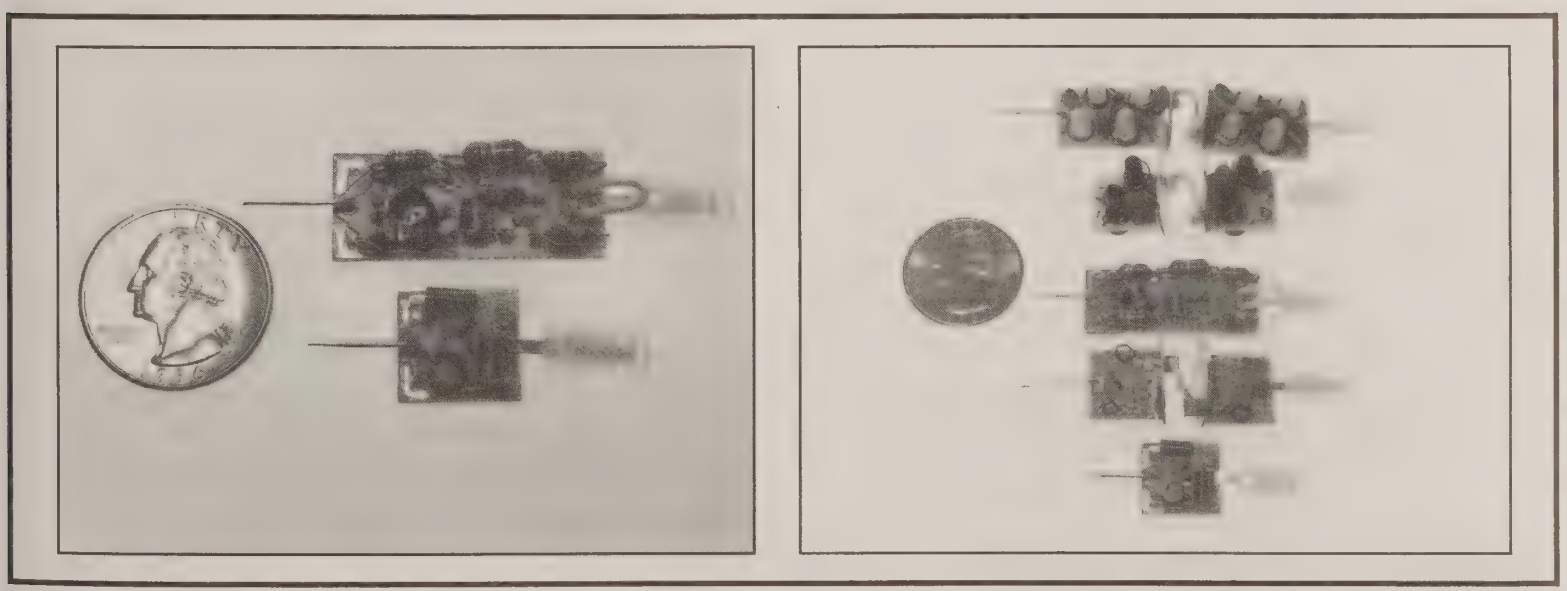
Circuit boards are produced on sheets and then broken apart to fit inside the cylinders. (Photo by C & E Corp.)

An Arcom quality control technician. Some firms such as Arcom check one hundred percent of their products rather than relying upon statistical methods. (Photo by C & E Corp.)

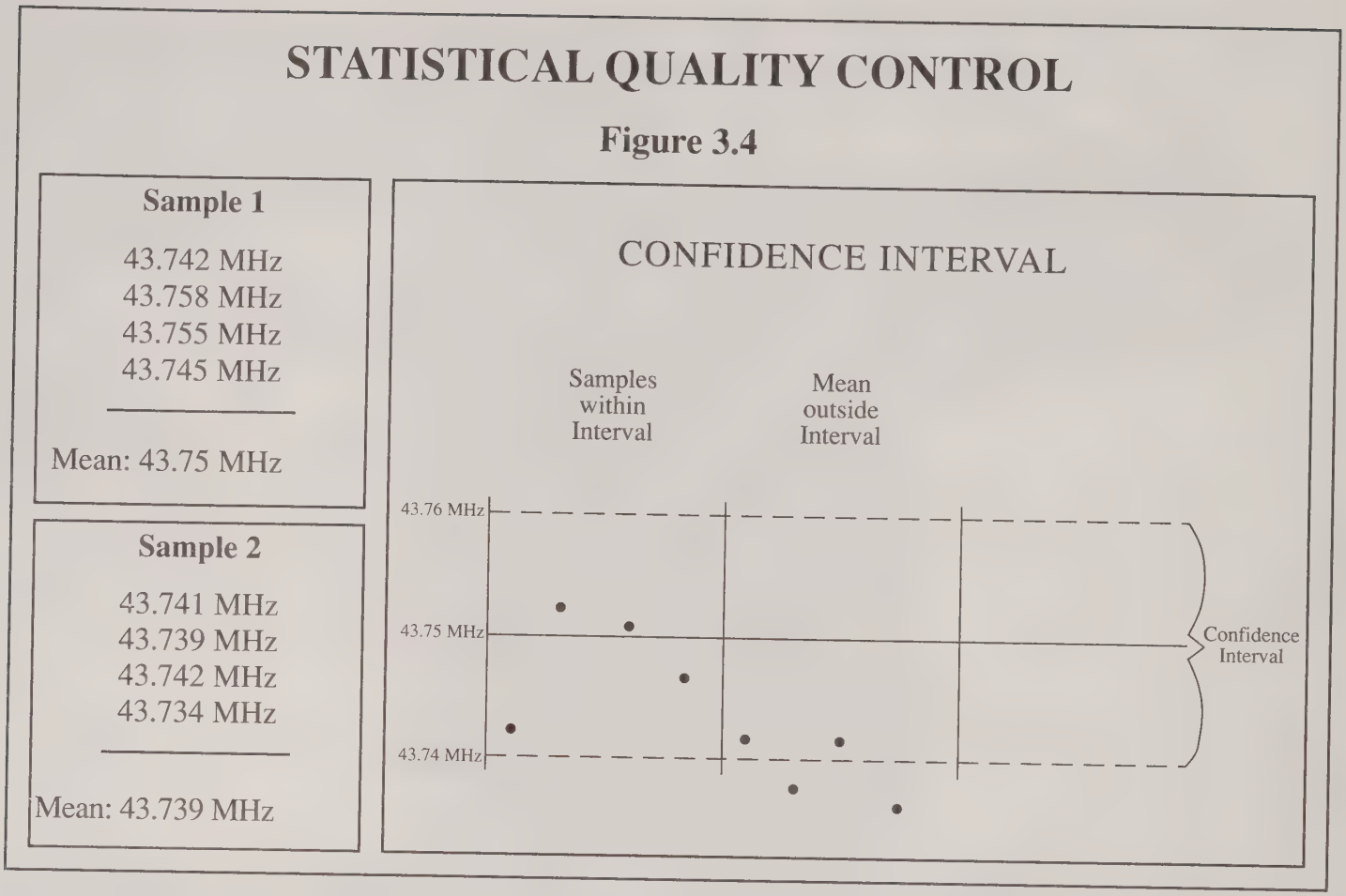
produced in large sheets with several hundred boards on a sheet. Capacitors and inductors are inserted into holes in the circuit board on a production line. Leads are soldered using a flow process. After soldering, the protruding leads are sheared away in one operation. The circuit boards are then snapped apart and placed in metal cylinders. A female Type F connector is integrated into one end of each cylinder. This avoids soldering two piece connectors. The cylinders have holes drilled in them for tuning purposes. Metallic tuning screws are inserted into coils though the holes.

Prior to tuning, each cylinder is filled with a polyurethane foam. This foam expands and packs every cavity of the filter. The form serves two purposes. First, it moisture seals the components. Second, the foam makes the filter more shock resistant.

After the foam has cured, the filters are tuned through the holes using an insulated non-metallic tuning tool. Next, the first (inner) cylinder is placed inside another (outer) protective cylinder. Two insulating gaskets are placed in each end of the cylinder and the outer cylinder is crimped to weather seal it. The outer cylinder is usually made of a nickel plated copper-brass alloy which resists damage and corrosion. It has a female Type F connector integrated into it. Thus, the finished product has a male connector at one end and a female connector at the other end.



Typical Arcom circuit boards before being placed inside the inner cylinders. (Photo by C & E Corp.)



Quality Control

Since pay television filters are mass produced, quality control is very important. The only way to insure that every trap works is to test every trap as it comes off the production line. Unfortunately, this procedure increases both production costs and filter prices. Thus, many filter manufacturers resort to statistical quality control methods. However, a few manufacturers (including *Arcom*) still test all traps coming off their assembly lines rather than gambling with quality.

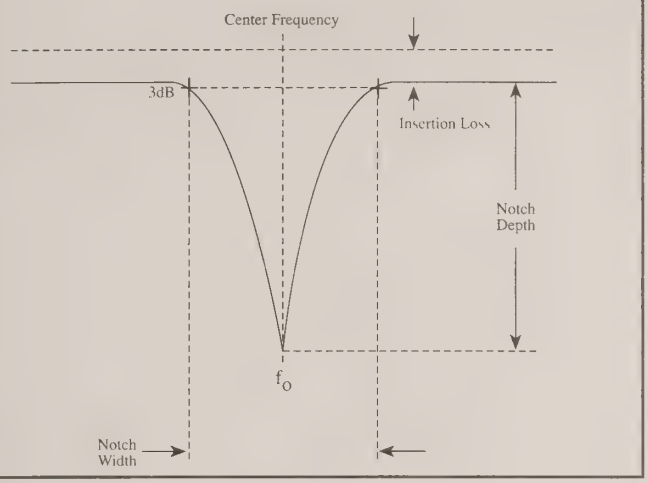
Because there are a variety of random influences in the production process, no two filters are ever exactly identical. Thus, the manufacturer seeks to maintain the characteristics of the product within specified tolerances. Because the actual value of each filter's specified parameters will vary from one filter to the next, the average or *mean* value of each specified parameter will vary from one batch to the next. This does not matter as long as the variations are within specified tolerances. Thus, the manufacturer only needs to be able to detect significant variations which will influence performance. This can be done statistically.

Using a valid statistical sample, the manufacturer can determine whether an average value associated with a production run varies significantly from the desired mean. Although the average value of parameters may vary from one batch to the next, the standard deviation of these variations should remain about the same from one run to the next. Using a statistical formula with a known standard deviation, it is possible to determine the size of the statistical sample needed to properly represent the filters in a specific production run. Further, this estimate can be done with a specified level of confidence. For example, the confidence level chosen could be 65-percent, 75-percent, 90-percent, 95-percent, or 99-percent. The higher the confidence level selected, the larger the sample needed.

Confidence intervals are calculated for specific statistical distributions by knowing the area under a normal curve between specific values. For example, approximately 68-percent of a normal distribution will lay within one standard deviation of the mean. Approximately 95-percent of a distribution will lay within two standard deviations of the mean. And approximately 99.7-percent of a normal distribution will lay within three standard deviations of the mean.

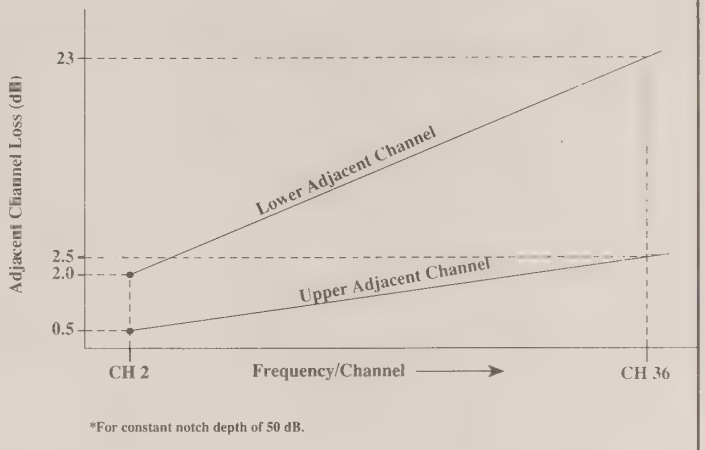
FILTER SPECIFICATIONS

Figure 3.5



ADJACENT CHANNEL LOSS VS. NOTCH FREQUENCY

Figure 3.6



*For constant notch depth of 50 dB.

Using a statistical formula, it is possible to establish a specific confidence interval for each specified parameter. For example, the 90-percent confidence interval for the frequency of a trap might extend from 73.74 MHz to 73.76 MHz if the specified value is 73.75 MHz. Hence, it is possible to check the frequency variations of traps to determine whether they are within the 90-percent confidence interval. If they are, one can be 90-percent confident that the actual mean is within the interval extending from 73.74 MHz to 73.76 MHz.

In order to obtain a *valid* representative sample, quality control personnel must take a random cross sectional sample of the filters coming off the production line. For example, the formula might indicate that a run of 10,000 filters with a known standard deviation requires a sample of one-hundred filters. If quality control personnel selected every 100th filter they would obtain a cross-sectional sample but it would not be random. Thus, for each batch of one hundred, they could select a random number between one and one-hundred to choose the sample filter. This can be done using either a random number table or a random number generator on a hand calculator.

Once a sample filter is selected, all specifications for that filter are checked and compared with the confidence intervals calculated for each parameter. If all parameters are within the interval, the batch of one-hundred is passed. However, if any parameter is outside the required confidence interval, all specifications are checked for all filters in the batch. This might indicate some systematic problem in the production process. For example, a malfunction in a spectrum analyzer could knock the analyzer *out of calibration* without anyone being aware of the problem. Bad filters in the suspect batch are tossed out and good filters are saved for sale. As each batch is passed, quality control personnel maintain a record of the values measured so that they can estimate mean parameters for the entire run.

Filter Specification

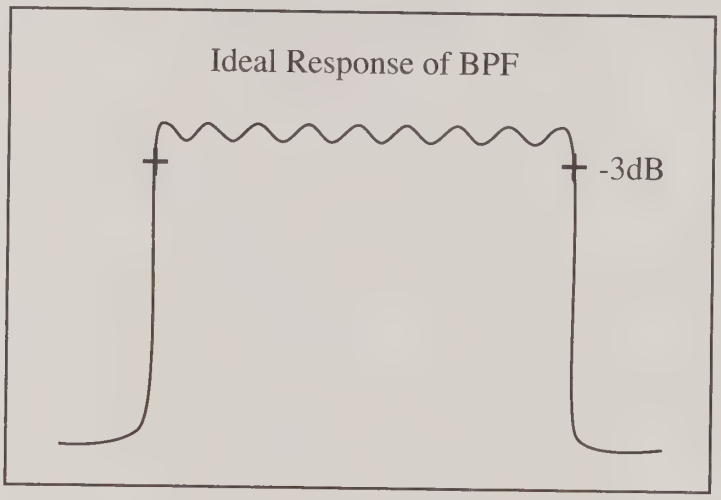
A variety of standardized conventions have been developed for specifying the performance of filtering devices. *Passbands*, *stopbands*, and *cut-off frequencies* are usually specified in MHz at their half-power or 3.0 decibel (dB) points. Half-power points are chosen because one must double the power output of an electronic device to produce a change which is perceptible by the human senses. Thus, one must half the power output to produce a perceptible reduction. Hence, filter *bandwidths* are usually measured in MHz at the 3.0 dB points.

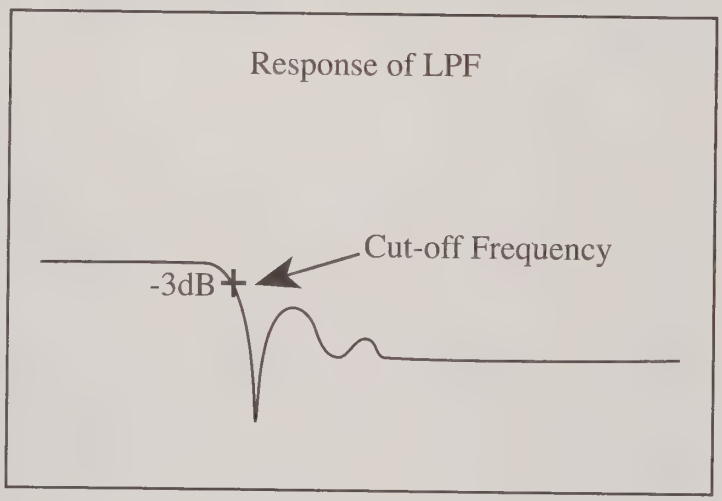
Filter suppression for a particular stopband is usually given in decibels (dB) as either a "minimum" or "typical" figure. Notch suppression is usually specified at the notch center frequency (f_o). The selectivity of a bandpass filter may be specified in decibels (dB) at a specific frequency in relation to the filter's center frequency (f_o +/- f).

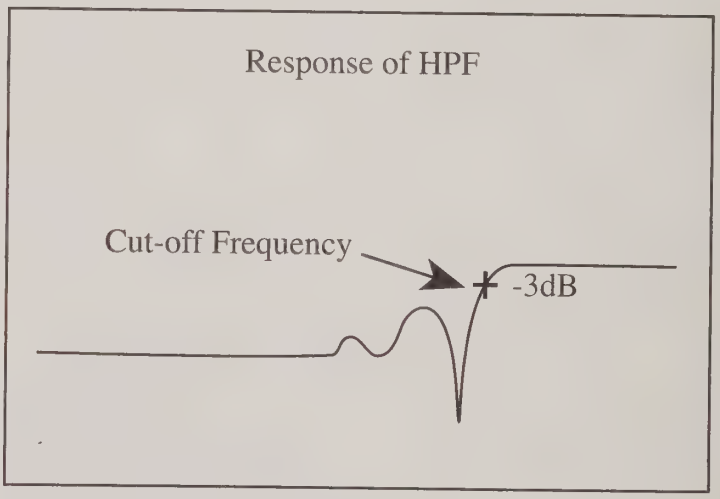
Passband insertion loss is usually given in dB as either a "minimum" or "typical" figure. With pay

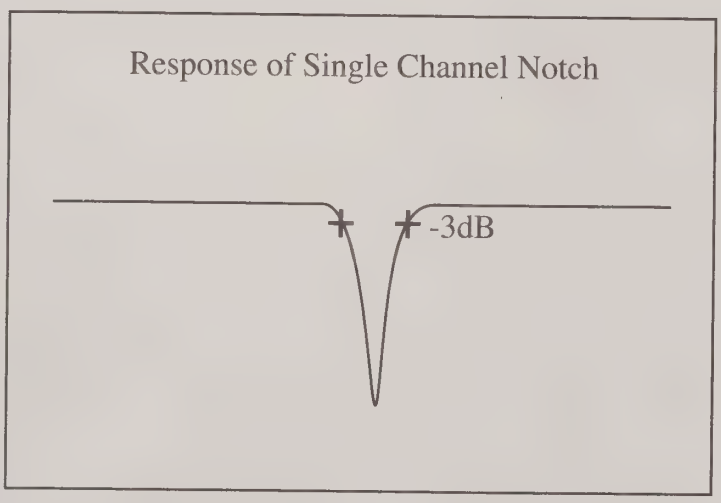
TYPES OF PAY TELEVISION FILTERS

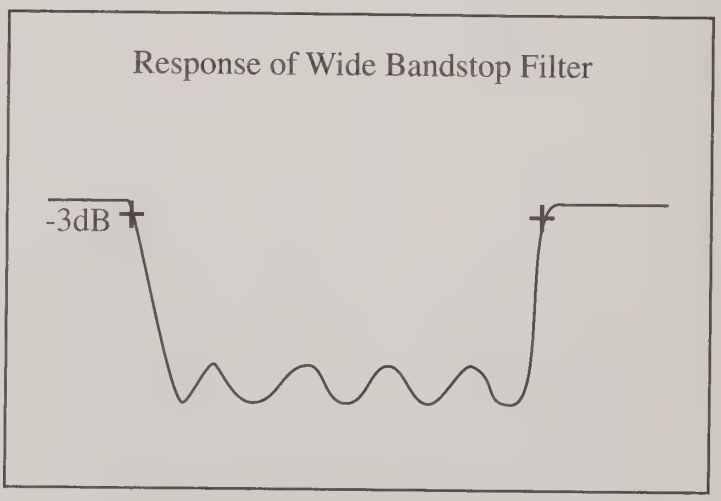
Figure 3.7











television traps, the amount of loss on adjacent channels is very important. Thus, the insertion loss for pay filters is usually specified for the adjacent channels. Ideally, the *lower adjacent aural carrier* and the *upper adjacent visual carrier* should not be significantly influenced by a trap.

Classification

It is not uncommon to find cable installers and manufacturers calling any cylindrical pay television filter a "trap" regardless of whether the filter is a bandpass filter, bandstop filter, highpass filter, or low-pass filter. Although this kind of informal slang is common, technically a "notch" filter or "trap" is a specific type of radio frequency filter. In general, radio frequency filters may be classified as either - (1) *lowpass filters* (LPFs), (2) *highpass filters* (HPFs), (3) *bandpass filters* (BPFs), or (4) *bandstop filters* (BSFs). Bandstop filters (BSFs) may be subdivided into two categories - (a) *narrow* bandstop filters, and (b) *wide bandstop* filters. Single channel "notches" or "traps" are actually narrow bandstop filters. "Tiering traps" are usually wide bandstop filters. However, HPFs, LPFs, or BPFs may also be used as tiering filters.

Performance Characteristic & Capabilities

In general, overall filter performance degrades as frequency increases. This is due to the inherent characteristics of the capacitors and inductors used to make pay television filters. In theory perfect inductors and capacitors have no resistance. However, in reality all electrical components have some resistance. The resistance in coils and capacitors degrades their performance. Engineers measure the quality of coils and capacitors using a *figure of merit* (Q). The quality (Q) of a coil or capacitor is the ratio of its reactance to its resistance. Thus:

[1] $Q = X_L / R_L = X_C / R_C$, where:

X_L = the inductive reactance of the coil

R_L = the resistance of the coil

X_C = the capacitive reactance of the capacitor, and

R_C = the terminal resistance of the capacitor.

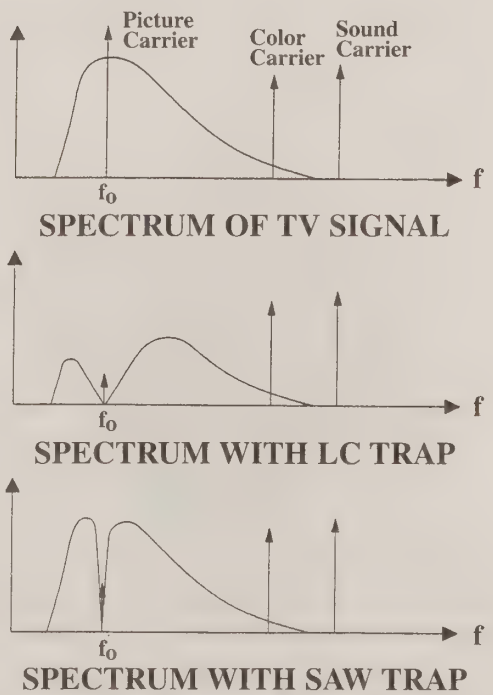
As frequency increases, the *composite figure of merit* of a filter declines. This has certain performance implications. Given a fixed notch depth, the width of a filter's stopband increases with an increase in notch frequency. As a result, adjacent channel loss increases as notch frequency increases.

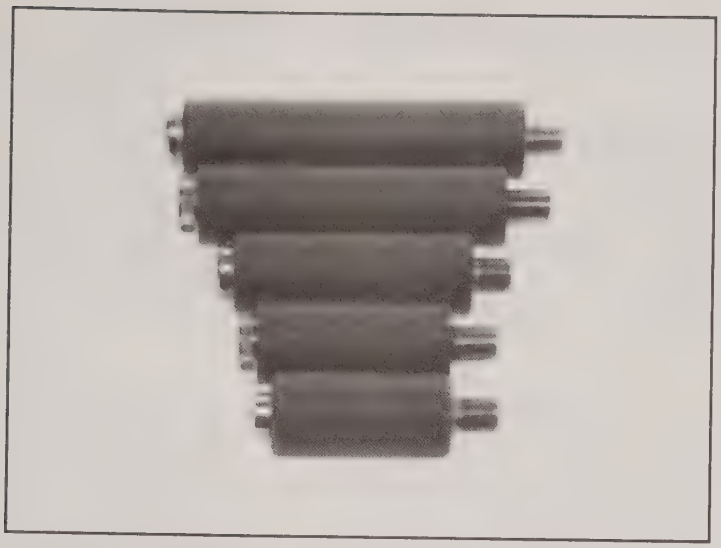
There are physical limits to what one can do with cylindrical filter designs. As notch frequency increases, it becomes more and more difficult to maintain low loss on the adjacent channels. Also, as notch frequency increases it becomes more and more difficult to maintain low loss at high passband frequencies. Filters made using "lumped constant" circuits also have secondary responses at multiples of their resonant frequency. For example, a basic bandpass filter with a resonant passband centered at 80 MHz will have a secondary passband at 160 MHz unless additional circuits are built into the filter to suppress the secondary responses.

Although filter manufacturers make specialized traps optimized for higher frequencies, it is more difficult to achieve higher selectivity at higher frequencies using discrete component technology.

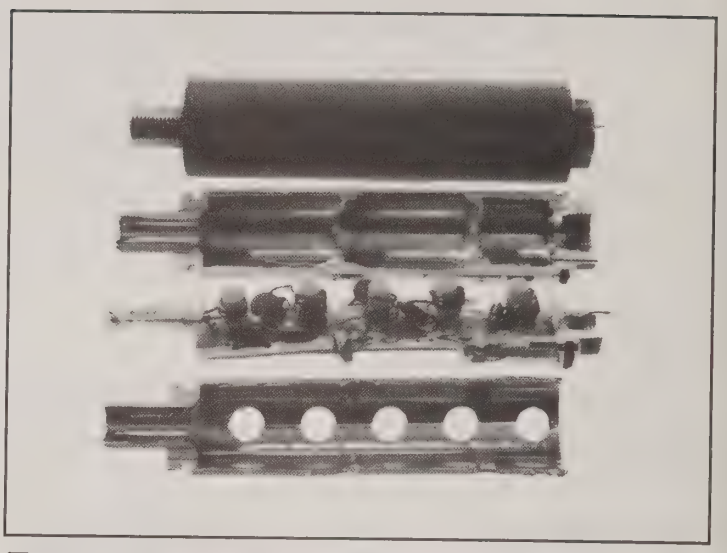
CONVENTIONAL LC TRAP vs. SAW FILTER
(Courtesy of Arcom)

Figure 3.8





Cylindrical filters are made in a variety of different sizes. (Photo by C & E Corp.)

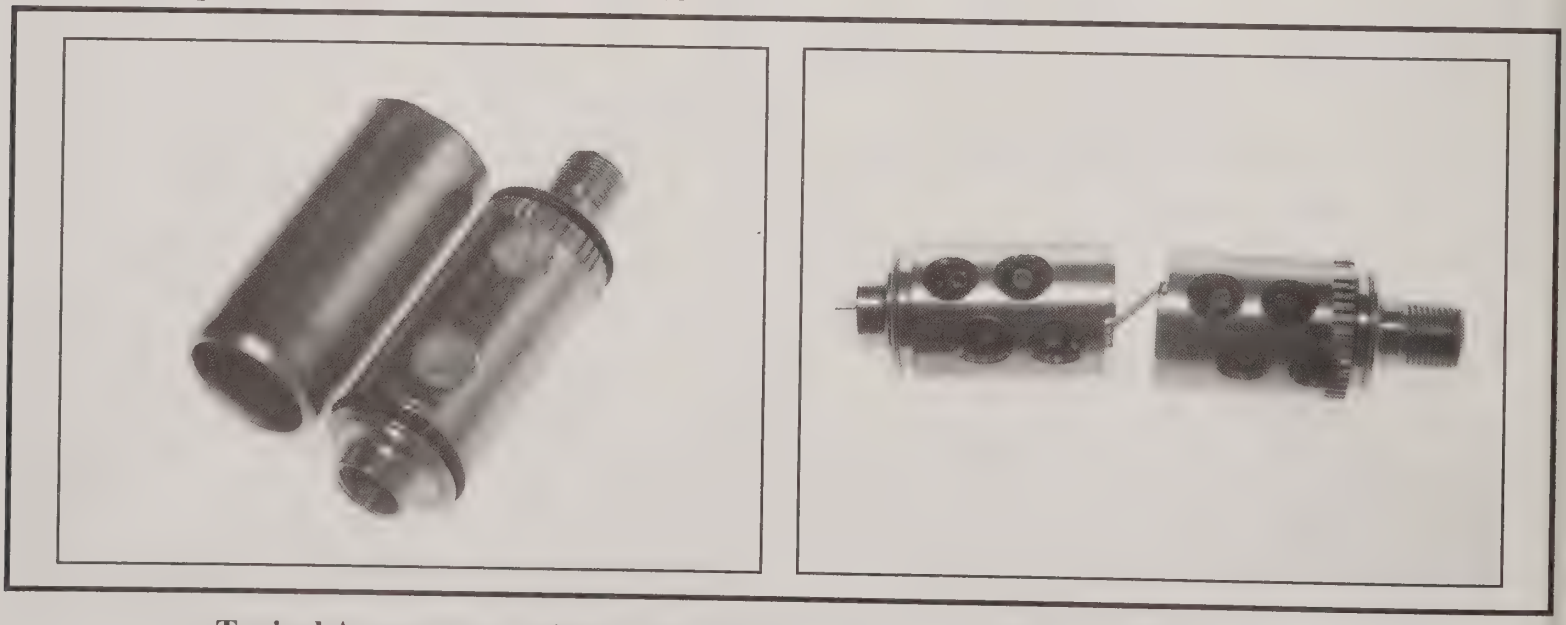


Traps are factory tuned through tuning holes in the inner cylinder before the assembly is placed inside the outer cylinder. (Photo by C&E Corp.)

Major performance improvements at higher frequencies must await the adoption of a *superior technology.* One such technology might be *surface acoustical wave* (SAW) technology. SAW technology has demonstrated the ability to produce very narrow bandwidths at frequencies up to 1.0 GHz. Development of pay filters based upon SAW technology would permit operators to trap individual channels throughout the UHF band. *Arcom Laboratories* is currently conducting research in this area. Results indicate that SAW technology is capable of achieving one tenth the bandwidth of an I C filter with the same notch depth at the same frequency.

Given the physical limits of cylindrical filters one might wonder how many filters can be connected in series on a tap? The answer is a function of five variables - (1) the insertion loss of the filters, (2) tap levels, (3) the sensitivity of a television receiver, (4) drop-line loss, and (5) the physical length of the filter.

The sensitivity of a typical television receiver is usually around - 30 dBmV. Tap levels usually average around + 12 dBmV. Although some traps have insertion losses of less than 1.0 dB, suppose that the average passband insertion loss for pay television filters ranges from 1.5 dB at the lower end of the band to 2.5 dB at 1 GHz. Drop-line loss is a function of cable length, connector losses, and any losses in the ground block.



Typical Arcom traps without outer cylinder covers. (Photo by C & E Corp.)

Although the specified insertion loss of coaxial cable varies from one manufacturer to another, the loss for RG-6 usually ranges from 1.6 dB at 54 MHz to 7 dB at 1 GHz. If one assumes a 75 foot length of RG-6, cable loss will range from 1.2 dB to 5.25 dB. If one assumes that the losses associated with connectors and the ground block amount to a maximum loss of around 1.0 dB, then drop-line loss can be estimated to average between 2.2 dB and 6.25 dB. If we assume that four filters are placed in series with each other, then the maximum average signal levels at the subscriber's receiver may be estimated as:

[2] 12 dBmV - 4 (1.5 dB) - 2.2 dB =

12 dBmV - 6 dB - 2.2 dB = + 3.8 dBmV

[3] / ∴ + 3.8 dBmV > - 30 dBmV

Similarly, minimum average signal levels may be estimated as:

[4] 12 dBmV - 4 (2.5 dB) - 6.25 dB =

12 dBmV - 10 dB - 6.25 dB = - 4.8 dBmV

[5] / ∴ - 4.8 dBmV > -30 dBmV

From inequalities [3] and [5] above it is clear that a 75 foot RG-6 drop-line will easily tolerate the insertion losses associated with four traps.[3] This is pretty much the experience reported by cable operators who regularly use up to four traps in series on a tap without any problems. This is especially true since the worst case estimates (above) assume an average tap output of + 12 dBmV. Tap output levels are sometimes as high as + 20 dBmV.

Beyond the issue of the maximum insertion loss which a drop-line will tolerate, *there is a physical limit to how many traps may be connected in series* with each other. The more traps one connects in series, the easier it is for a pirate to break them off. Thus, using more than four traps in series becomes physically problematic.

Although there have been many technological advances since the inception of cable television, much remains the same. The basic outlines of cable's war with "pirates" have not changed. Filter technology continues to provide an effective and inexpensive means of securing premium programming for cable operators throughout the United States and the world.

[3]Set-top converters are purposely designed to be less sensitive than television sets designed for broadcast reception. Most set-tops like to "see" 0 to - 6 dBmV at their inputs. In cases where drop-line loss becomes a problem on long lines, some operators use a + 10 dB tubular amplifier. *Pico Products Inc.* and a number of others make such line amplifiers.

Works Consulted

American Radio Relay League, ***The Amateur's Handbook.*** 46th Edition. Doug. DeMaw, ed. Newington, CT.: American Radio Relay League, 1969.

Arcom CATV Products, "DN, TN Series Multi-Channel Double Density Negative Traps" [Informational Monogram]. Syracuse, New York: Arcom CATV Products, nd., pp. 1-5.

Arcom CATV Products, "Double Density Tiering Traps" [Informational Monogram]. Syracuse, New York: Arcom CATV Products, nd., pp. 1-5.

Arcom CATV Products, "DN Series Double Density Mini Negative Traps" [Informational Monogram]. Syracuse, New York: Arcom CATV Products, nd., pp. 1-3.

John E. Cunningham, ***Cable Television.*** 2nd Edition. Indianapolis, Indiana: Howard W. Sams & Company, 1983, pp. 11-19.

Eagle Comtronics, Inc. "History of Cable Television Relating to Traps & Filters" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd, pp. 1-4.

Eagle Comtronics, Inc., "How Negative Traps Work" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "How To Select a Trap for Premium Channel Control" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "Micro Series Negative Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "One GHz Negative Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "Eagle Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-3.

Eagle Comtronics, Inc., "Ultra Narrow Negative Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Federal Communications Commission, "Part 76" in Office of the Federal Register, National Archives and Records Division, ***Title 47 Code of Federal Regulations, Parts 70 to 79.*** [Revised October 1, 1995] Washington, D.C.: U.S. Government Printing Office, 1995.

William Grant, ***Cable Television.*** 1st edition. Reston, Virginia: Reston Publishing Company, Inc. 1983), pp. xiii - xx.

John Gutierrez, "RF Leakage Testing Using A Simple Test Chamber" in ***Communications Engineering Design.*** February 1989. pp. 87, 88, 89.

International Telephone and Telegraph, ***Reference Book for Radio Engineers.*** New York: Howard W. Sams & Company, Inc. 1991.

George L. Matthaei, Leo Young, and E.M.T. Jones. ***Microwave Filters, Impedance-Matching Networks, and Coupling Structures.*** Dedhem, MA: Artech House Books, 1980.

David S. Moore and George P. McCabe, ***Introduction to the Practice of Statistics.*** New York: W.H. Freeman and Company, 1989.

Pico Products, Inc., "Collected Filter Specifications & Spectrum Plots" [Loose leaf collection of photocopied spectrum plots and product information provided by manufacturers representative]. Liverpool, New York: Pico Products, Inc., nd [1994].

Donald R.J. White, ***A Handbook On Electrical Filters: Synthesis, Design, and Application.*** Gainesville, Virginia: Don White Consultants, Inc., 1980.

Anatol I. Zverev, ***Handbook of Filter Synthesis.*** New York: John Wiley & Sons, 1967.

Chapter 4
Negative Filtering

Negative filtering is one of the oldest, most secure, and least expensive program security methods. Despite the introduction of more sophisticated methods - which have sometimes proven less secure - negative filtering has survived because it is *effective and inexpensive*. With increasing competition from Direct Broadcast Service (DBS), Wireless (MDS/MMDS) Television, Multi-channel Low Power Television (LPTV), and Digital Broadcast Television; cable operators continue to need some *inexpensive* and effective way of securing their programming.

Key Specifications

In general, negative filters may be divided into two categories - (1) *single channel traps*, and (2) *tier filters*. The former secure individual premium channels while the later secure whole groups of pay channels. Regardless of whether a negative filter is a single channel trap or a tier filter, four key specifications heavily influence filter performance - (1) *passband*, (2) *passband insertion loss*, (3) *stop-band suppression*, and (4) *adjacent channel loss*.

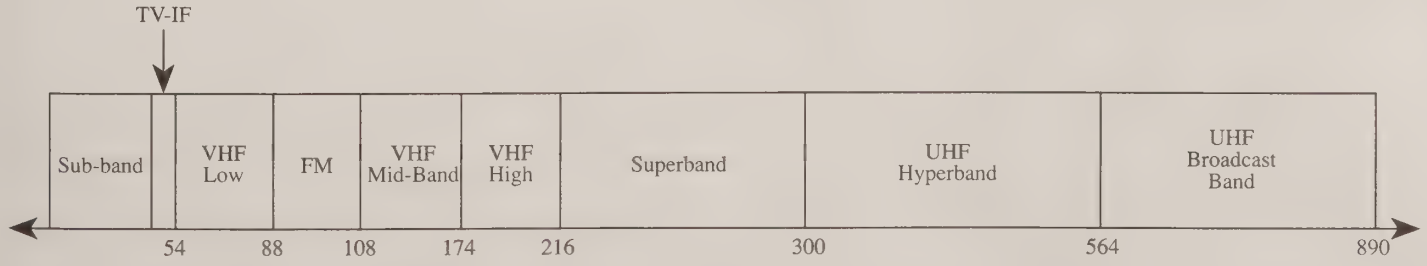
Passband. The passband of a filter is important because it limits *how many other channels* a subscriber can receive. The cable television spectrum (between 54 MHz and 1 GHz) is made up of the VHF low band, the FM band, the VHF mid-band, the VHF high band, the super band, and the hyperband. If a cable operator only uses the spectrum between 54 MHz and 535 MHz for a seventy-five channel system, then (with the exception of the filter stop-band) the filter should have a low passband insertion loss up to 535 MHz in order to pass all of the other cable channels. However, this leaves no room for future expansion. Should the operator decide to add channels, an even wider passband would be needed. Thus, practical pay television filters should have minimum insertion loss between 54 MHz and 1 GHz. For this reason, a passband of 54 MHz to 1 GHz has become the *de facto* standard for pay television filters.

Passband Insertion Loss. Passband insertion loss influences signal levels on desired channels. A passband insertion loss of less than 1.5 dB will not be perceptible to viewers. However, because it is seldom possible to keep insertion losses below 1.5 dB at frequencies as high as 900 MHz, losses as high as 2.5 dB are sometimes tolerated.

In general, insertion loss on a coaxial cable increases with frequency. This is called "line-tilt." Older cable systems used passive equalization networks in their trunk amplifiers to correct for line-tilt. Today, most cable systems have *automatic slope control* (ASC) systems to correct for line-tilt on trunk lines. However, because most coaxial devices have some degree of "line-tilt," it continues to be a factor with filters and drop-lines. It becomes increasingly difficult to maintain low insertion loss as the bandwidth and passband frequency of a filter increases. A filter with a passband of 54 MHz to 1 GHz will be more complex and expensive than a filter with a passband of 54 MHz to 300 MHz.

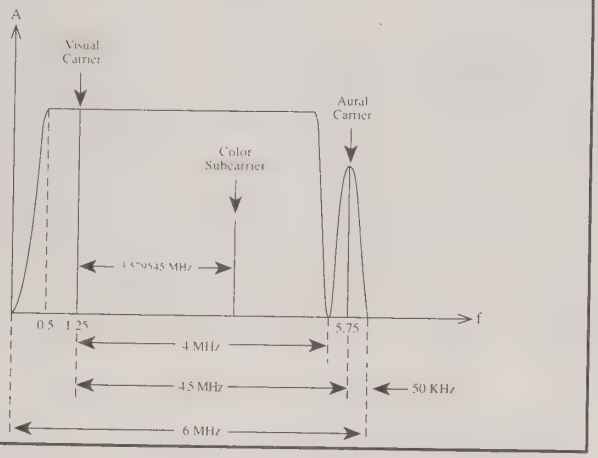
THE CATV SPECTRUM

Figure 4.1



NTSC TELEVISION CHANNEL

Figure 4.2



Stopband Suppression. Stopband suppression is important because it determines whether the subscriber can receive an unauthorized channel. Suppression requirements for negative filters are determined by four factors - (1) carrier-to-noise ratio requirements, (2) receiver sensitivity, (2) tap levels, and (4) temperature sensitivity.

In general, the television industry recognizes a carrier-to-noise ratio of 45 dB as the minimum standard for quality analog television reception. The threshold sensitivity of television receivers is typically - 30 dBmV (30 dB below 1.0 mV). Signal levels at the input to subscribers' drop-lines are usually around + 12 dBmV. Thus, in theory a notch suppression of 45 dB should be sufficient to protect premium channels:

[1] 12 dBmV - 45 dBmV = - 32 dBmV

[2] /∴ - 32 dBmV < - 30 dBmV

However, for single channel pay traps, higher levels of suppression may sometimes be desirable *on visual carriers* . In fact, it is not uncommon to find negative channel traps with notches of 70 dB or more. The reasons can be understood when one realizes that the tap level used in the foregoing calculation was only an *average level.*

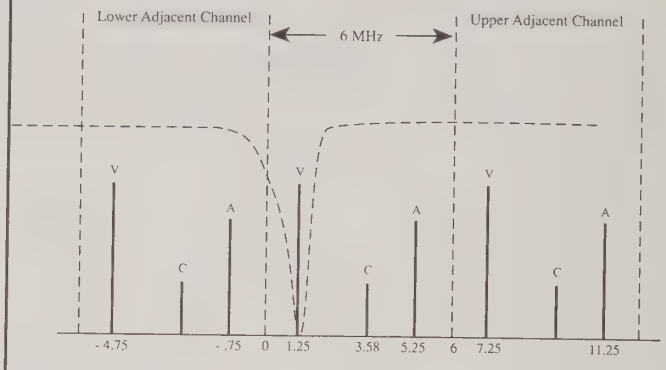
Some cable taps have levels as high as 20 dBmV. In that event:

[3] 20 dBmV - 45 dBmV = - 25 dBmV

[4] / ∴ - 25 dBmV > - 30 dBmV

ADJACENT CHANNELS

Figure 4.3

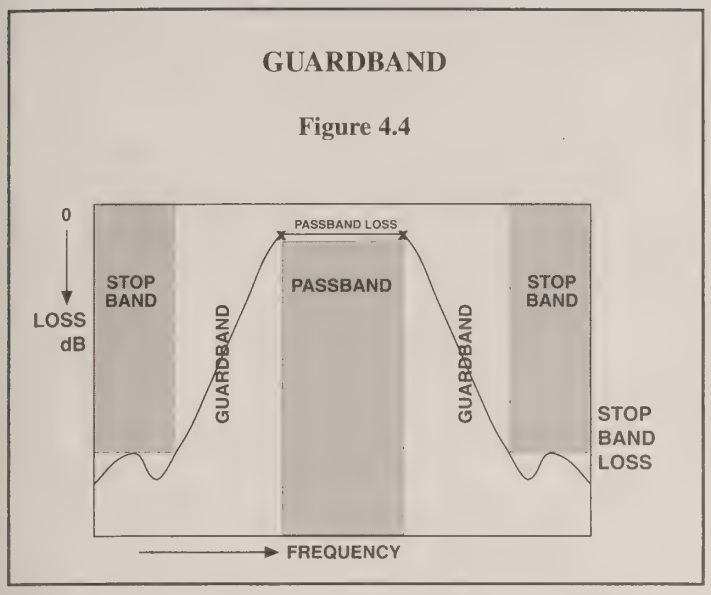


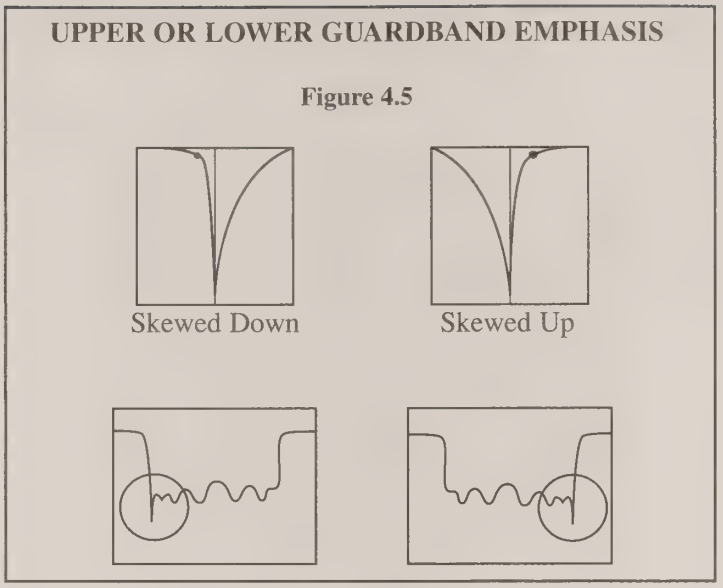
Thus, suppression levels of 55 to 60 dB may be desirable for single channel pay traps. However, in order to reduce the *temperature sensitivity* most filter manufacturers use deeper notches to widen the stop-band. Hence, notches of 70 dB or more are common.

Adjacent Channel Loss. The selectivity of a notch filter measures its ability to discriminate between desired and undesired frequencies. The higher the selectivity of a notch, the steeper its "skirts." A pay television filter should have minimum impact upon the upper and lower adjacent channels. Single channel traps should have high selectivity. In the previous chapter we saw that as notch frequency increases stopband width also increases. It becomes increasingly difficult to maintain low loss on the adjacent channels. Thus, as notch frequency increases, filter selectivity declines.

Adjacent channel loss is heavily influenced by the arrangement of NTSC channels within the cable spectrum. Because there are gaps between channels in certain parts of the television spectrum, the effect of adjacent channel insertion loss is mitigated in certain cases. For example, there are gaps in the television spectrum between VHF Channels 4 and 5. There may be additional gaps between channels depending upon the operator's channel arrangement.

Generally, higher losses can be tolerated on lower adjacent aural carriers than on the upper adjacent visual carriers. Adjacent channel losses on upper visual carriers of 3.0 dB will hardly be perceptible to the viewer. However, adjacent channel loss on the lower aural carrier may be as high as 10 dB without significant degradation. To understand why, one must





understand how receivers work.

NTSC television channels are 6 MHz wide. Each channel has three carriers - (1) an *Amplitude Modulated* (AM) visual carrier, (2) a color subcarrier, and (3) a *Frequency Modulated* (FM) aural carrier. A wide vestigial sideband carrier is transmitted at 1.25 MHz above the bottom edge of each television channel. This visual carrier contains information which the receiver needs to assemble a black and white television picture. The color subcarrier, located at 4.83 MHz between the visual and aural carriers, contains information used to make a color picture. The narrow FM aural carrier is transmitted at the top of the channel. In general, aural carriers are transmitted at 7 to 16 dB below the visual carrier.

Because AM signal detectors respond to *variations in signal level*, the wide visual carrier is much *more* sensitive to amplitude distortions than the FM aural carrier. Hence, visual carriers cannot tolerate as much loss as aural carriers.

Aural carriers are much *less* sensitive to amplitude distortions than visual carriers. There are four reasons for this. First, television receivers use *ratio detectors* or *discriminators* to demodulate frequency modulated audio signals. These FM devices respond mainly to frequency variations. Second, the aural carriers used by television receivers are relatively narrow. Because FM aural carriers are narrow, amplitude variations caused by filters usually have less impact than would be the case over a wider bandwidth. Aural carriers are only 50 KHz wide. Third, FM carriers are normally transmitted at much lower levels. Finally, the audio section of a television receiver contains an *automatic gain control* (AGC). The AGC will tend to compensate for low audio levels. Thus, aural carriers are much less sensitive to amplitude distortions than visual carriers.

Guardbands. The transition between a filter's passband and stopband is never instantaneous. Filters have skirts which "roll-off" between the passbands and stopbands. The width of the guardband influences the selectivity of the filter. It also heavily influences adjacent channel loss. In designing filters it is usually possible to emphasize either the front or back end of the guardband in order to place a lower loss on either the lower aural carrier or the upper visual carrier. As previously indicated it is usually desirable to place lower loss on the upper visual carrier. However, *there are exceptions.* If the spectrum above a specific channel is vacant, then one might want to emphasize the lower aural carrier.

Channel Traps

Single channel pay traps are used for protecting premium channels. These programs are usually movie channels like *HBO* or *Cinemax*. Subscription rates typically run around $ 10.00 per month. The cable operator simply places traps in the drop-lines of non-subscribers.

As we saw in previous chapters negative traps work by trapping out visual carriers. Without the visual carrier, a television receiver cannot assemble a basic black and white picture. To be effective a single channel notch filter must have a notch depth of

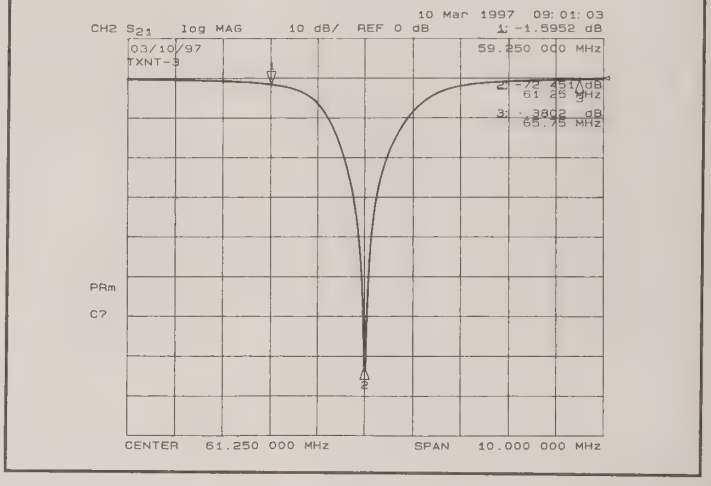
45 to 60 dB. However, negative traps typically have notches of 70 dB or more to help reduce their temperature sensitivity. Usually a four pole filter is sufficient to achieve a notch of 60 or 70 dB with reasonable selectivity. Although exact filter specifications vary from one filter manufacturer to another, the specifications shown in Table 4.1 are typical.

Split-Tuning. It is possible to tune the sections of a negative filter to place *separate notches* on selected carriers instead of having only one notch on the visual carrier. For example, seperate notches can be placed on the visual carrier and the aural carrier. Alternatively, it is possible to put a separate notch on the visual, color, and aural carriers by tuning different filter sections to each frequency. Since aural and color carriers are broadcast at lower levels than the visual carrier, shallower notches are sufficient to completely obliterate them. However, the receiver may still be able to assemble a black and white picture without the audio. Nevertheless, this type of arrangement has applications at frequencies where it is necessary to save the adjacent channels.

Multi-Channel Traps. Individual channel traps may be connected in series to secure more than one pay channel. The only limits on the number of traps which may be connected in series is the amount of additional passband insertion loss which the drop-line will tolerate on the highest channel in the system and the physical length of the filter. As we saw in the previous chapter, this limit is usually around four traps.

FREQUENCY RESPONSE OF TYPICAL NEGATIVE TRAP
(Courtesy of Arcom)

Figure 4.6



In order to minimize the insertion loss of multiple filters, it is possible to build more than one trap into the same enclosure. This eliminates the insertion losses associated with the additional F connectors and allows the factory to optimize the filters at the time they are tuned.

Performance Characteristics. We saw in the previous chapter that filter Q limits the performance of filters made with discrete components. Given a fixed notch depth, Table 4.2 illustrates what happens to the adjacent channels as the notch frequency of a

SINGLE CHANNEL NEGATIVE TRAPS

Typical Specification

(Channel 13)

Table 4.1

Passband:	0 to 1 GHz
Passband Insertion Loss:	- 2.5 dB (maximum)
Stop Band Suppression:	- 75 dB (maximum)
Adjacent Channel Loss:	
- Lower Aural Carrier:	-9.5 dB (typical)
- Upper Visual Carrier:	- 1.5 dB (typical)
Operating Temperature:	-40 to + 140 degrees Fahrenheit
RFI/EMI Isolation:	> 100 dB
Power Passing:	0.5 Amperes (maximum)
Input / Output Impedance:	75 ohm
Connectors:	Type F (male & female)
Diameter:	0.812 inches
Construction:	Polyurethane Foam Filled Double Sleeve

NEGATIVE TRAP PERFORMANCE

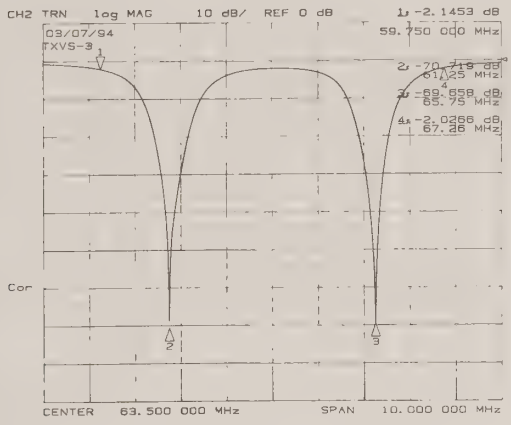
(Single Channel Trap)

Table 4.2

Notch Frequency (MHz)	Lower Aural	Trapped Aural	Upper Visual
50 - 190	Clear	Faint	Clear
190 - 220	Clear	Gone	Clear
220 - 275	Satisfactory	Gone	Clear
275 - 300	Noisy (Hisses)	Gone	Satisfactory
300 - 350	Very Faint	Gone	Satisfactory
350 - 400	Very Faint	Gone	Watchable
400 - 550	Not audible	Gone	Unwatchable

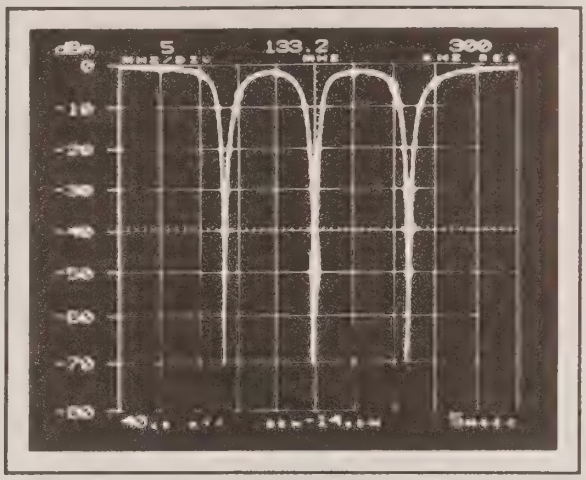
AURAL/VISUAL SPLIT-TUNING

Figure 4.7



FREQUENCY RESPONSE OF MULTICHANNEL TRAP
(Courtesy of Arcom)

Figure 4.8



single channel trap increases. Above 275 MHz the lower adjacent aural carriers become inaudible. Above 400 MHz, upper adjacent visual carriers become unwatchable. Thus, if one has to save the adjacent channels, one is limited to channels below 275 MHz. However, if one can sacrifice the lower adjacent channel, the limit may be extended to 400 MHz. This is one reason why any "gaps" in the CATV spectrum and "split-tuning" are significant for system designers.

Tier Filters

Tier filters block wider bands than single channel traps. They work by suppressing all or most of the signals for a whole group of television channels. In general, tier filters may be divided into four basic filter categories - (1) highpass filters, (2) lowpass filters, (3) wide bandstop filters, and (4) bandpass filter. Typically tier filters have between four and sixteen poles depending upon the width of the stop-band.

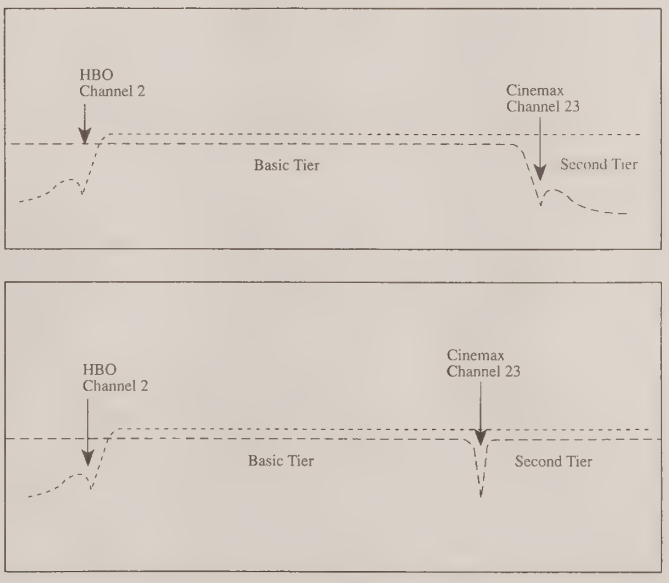
Tier filters perform two significant functions for cable operators. First, they allow cable operators to separate "basic" subscribers from those who subscribe to more costly pay services. Second, they allow cable operators to subdivide the more costly pay services into a variety of "program packages."

Many franchise contracts contain provisions which *require* cable operators to supply some "basic" level of service at a relatively low cost. This requirement is usually part of a contract negotiated with the local franchise authority at the time the franchise was sold. The *political motivation* behind this requirement is simply to insure that low income and retired subscribers have low cost access to some basic level of service.

Typically "basic" service will contain all local broadcast stations, a community access channel, and perhaps a local weather channel. Since most of these channels can usually be received with a set of rabbit ears or a roof top antenna, basic service tends to "bring in" customers which might not otherwise subscribe. At a relatively low cost basic customers can dispense with rabbit ears and roof top antennas and be assured of quality reception on all local channels. Rates for basic service are typically $ 5.00 to $ 7.00 per month. Hence, cable operators needed

NEGATIVE TIER FILTERING

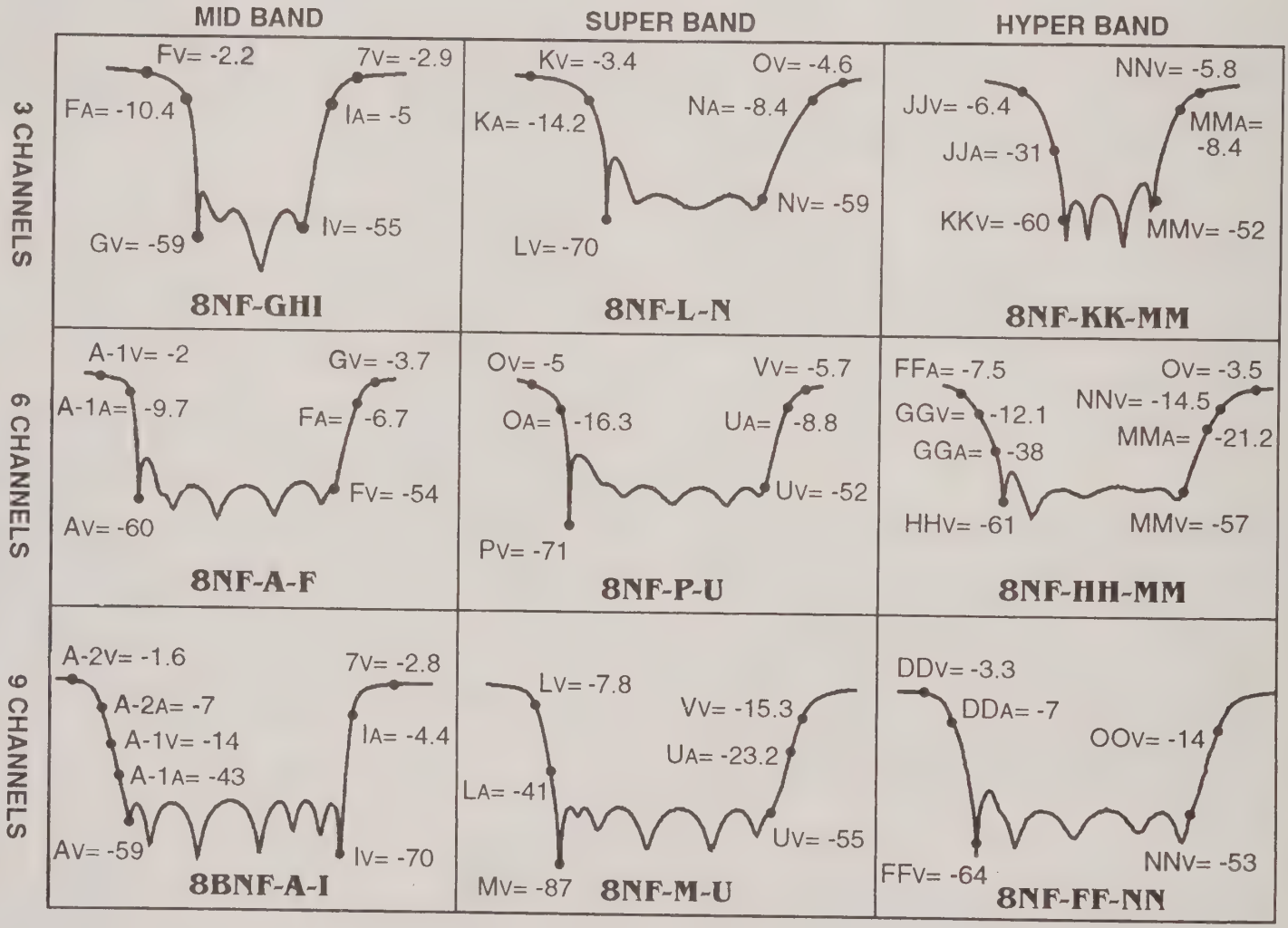
Figure 4.9



FREQUENCY RESPONSE OF TYPICAL TIER FILTERS

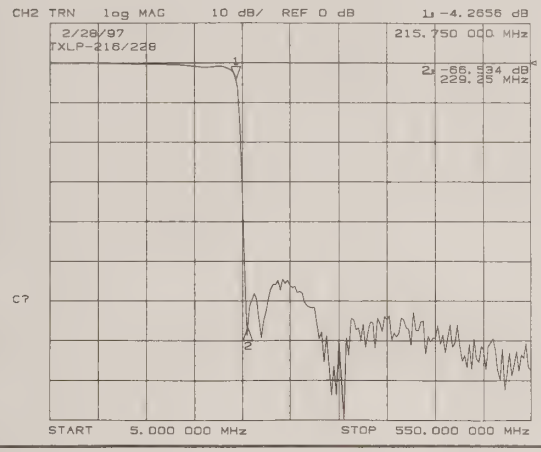
(Courtesy of Eagle Comptronics)

Figure 4.10



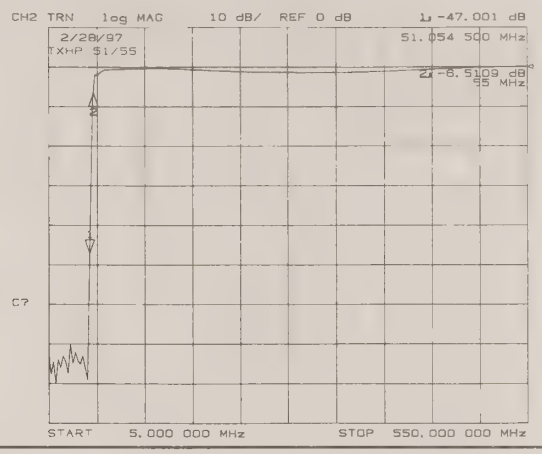
FREQUENCY RESPONSE OF LOWPASS TIER FILTER

Figure 4.11



FREQUENCY RESPONSE OF HIGHPASS TIER FILTER

Figure 4.12



some *inexpensive* way of separating these "basic" customers from those who subscribe to more costly pay channels. One way a cable operator can do this is by arranging all of the "basic" channels at the bottom of the cable spectrum. The more costly pay channels are placed further up the band. An *inexpensive* lowpass filter can then be used to block all of the more expensive channels to "basic" subscribers. Thus, the filter's stopband blocks all of the more expensive channels further up the band while the passband passes all of the basic channels at the bottom of the spectrum.

Some operators use this approach in conjunction with set-top converters for premium customers. Thus, a filter is used on the drop-line of all basic subscribers and a set-top converter is given to all subscribers who want a large number of premium movie channels. Because cable is so popular now, the population of basic subscribers in some systems is actually a minority of cable subscribers. Hence, a system with 45,000 subscribers may only need to buy 8,000 negative filters for their basic subscribers.

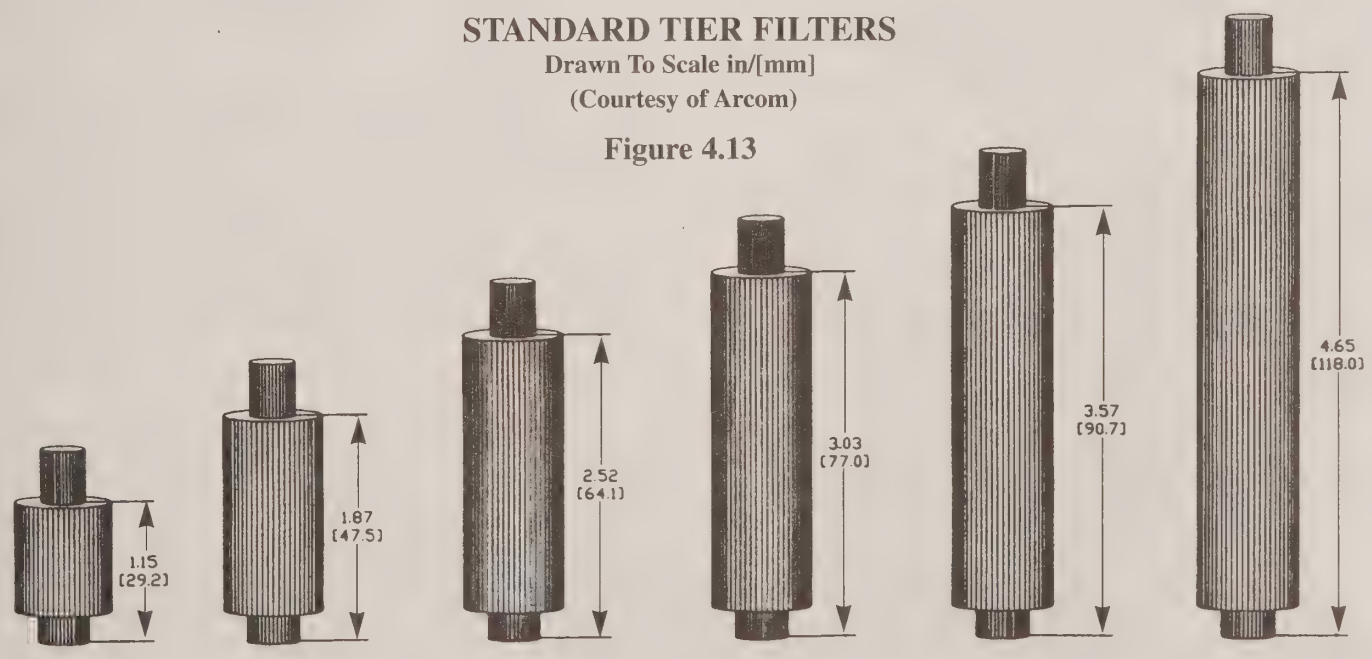
One advantage of this approach is that the security provided by a negative filter *adds* to any security provided in the set-top converter. Thus, if *HBO* is deciphered by the set-top converter, a basic subscriber who vandalized the pole in order to remove the trap would still not receive *HBO*.

STANDARD TIER FILTERS

Drawn To Scale in/[mm]

(Courtesy of Arcom)

Figure 4.13



Tier filters are also used for protecting groups of low cost *commercial* satellite channels. These are typically more specialized channels like *Nickelodeon*, *A & E*, the *Discover Channel*, or the *History Channel*. Typical subscription rates for such channels are around $ 0.50 to $ 0.90 per month per channel. Most subscribers do not watch such channels all of the time and will not pay a lot for them. They are not valued enough by average subscribers to be purchased individually at a high price. Nevertheless, subscribers will usually purchase such channels if they are grouped with other channels. A subscriber who may have a periodic interest in a specialized channel may want the channel if service is combined with a more popular commercial channel like *CNN*. Thus, cable operators can combine a number of less valuable commercial satellite channels and package them as a more valuable group.

Wide bandstop filters are manufactured as tiering filters to block either three, six, or nine channels at a time. Thus, a "non-basic" subscription tier may be subdivided in a variety of ways to provide a variety of subscription options. A wide variety of tier arrangements are possible using wide bandstop filters, bandpass filters, highpass filters, or lowpass filters in conjunction with various other security systems.

Works Consulted

Arcom CATV Products. "DN, TN Series Multi-Channel Double Density Negative Traps" [Informational Monogram]. Syracuse, New York: Arcom CATV Products, nd., pp. 1-5.

Arcom CATV Products. "Double Density Tiering Traps" [Informational Monogram]. Syracuse, New York: Arcom CATV Products, nd., pp. 1-5.

Arcom CATV Products. "DN Series Double Density Mini Negative Traps" [Informational Monogram]. Syracuse, New York: Arcom CATV Products, nd., pp. 1-3.

John E. Cunningham, ***Cable Television.*** 2nd Edition. Indianapolis, Indiana: Howard W. Sams & Company, 1983, pp. 11-19.

Eagle Comtronics, Inc., "How Negative Traps Work" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "How To Select a Tap for Premium Channel Control" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "Micro Series Negative Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "Multi-Channel Negative Tiering Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "One GHz Negative Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "Ultra Narrow Negative Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

William Grant, ***Cable Television.*** 1st edition. Reston, Virginia: Reston Publishing Company, Inc. 1983), pp. xiii - xx.

Gary M. Miller. ***Modern Electronic Communication.*** Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1983.

Pico Products, Inc., "Collected Filter Specifications & Spectrum Plots" [Loose leaf collection of photocopied spectrum plots and product information provided by manufacturers representative]. Liverpool, New York: Pico Products, Inc., nd [1994].

Chapter 5
Positive Trapping

In theory, if *all* of the customers on a cable system subscribed to a particular premium channel and the operator used negative trapping, the operator would not have to use any negative traps at all. However, in practice the number of non-premium customers usually exceeds the number of premium customers. As a result, a cable operator using negative filtering methods *must place a trap in the drop-line of everyone who does not subscribe* to the premium channel. The positive security system was developed to avoid this problem.

With positive security systems, the cable operator places a filter in the drop-line of *only those customers who subscribe* to the pay channel. Thus, if a cable system with 20,000 subscribers has only one premium customer, the operator need only purchase and install one trap. With the negative security system, the cable operator would have to purchase and install 19,999 traps. Hence, where penetration rates are low, positive security systems offer distinct financial advantages. For this reason, positive systems are very economical when penetration rates are low.[1] Positive trapping methods are also useful in small private cable systems with limited financial resources.

The Positive Security System

In general, positive security systems may be classified as either (1) discrete jamming systems or (2) pre-emphasis systems. Discrete systems may be sub-classified as either *"Radio Frequency"*(RF) *systems* or *Intermediate Frequency"* (IF) *systems*.

With RF systems the jamming carrier is inserted directly at the frequency of the television channel being jammed. IF systems insert the jamming carrier at an intermediate frequency level in the TV-IF band (41 MHz to 47 MHz).

The TEST Security System. The TEST Positive Security System was patented by James Tanner[2] on June 18, 1976 and eventually acquired by *Pico Products Inc.*[3] TEST is a discrete RF system because the jamming carrier is inserted into the television channel at RF level and filtered out in the subscriber's drop-line.

The original TEST system used an unmodulated jamming carrier 2.25 MHz above the visual carrier at 3.5 MHz. The level of the interfering carrier was transmitted at 0 dB with respect to the visual carrier. Later variations of the system used a 2.257 MHz interfering carrier. Thus, the jamming carrier falls 3.507 MHz above the lower edge of the television channel between the visual carrier and the color subcarrier. The 3.507 MHz carrier was *modulated at 80-percent* with a 15 Hz signal and a 1.0 KHz signal.

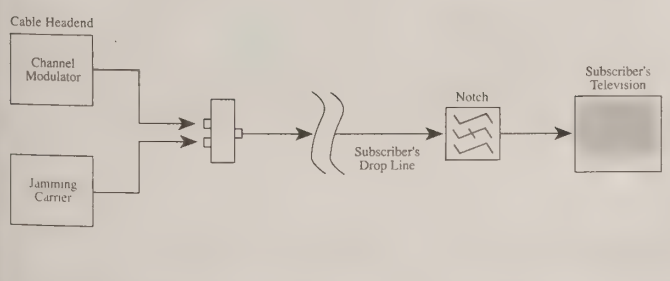
[1]A subsequent chapter will discuss the economics of filtering in greater detail.

[2]Patent No. 4,074, 311 issued February 14, 1978.

[3]Since Patents have a term of seventeen years, the Patent on the TEST Security Systems has expired and the system has entered the public domain.

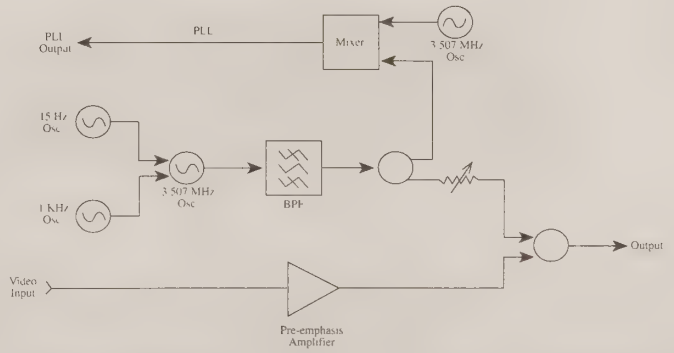
THE POSITIVE SECURITY SYSTEM

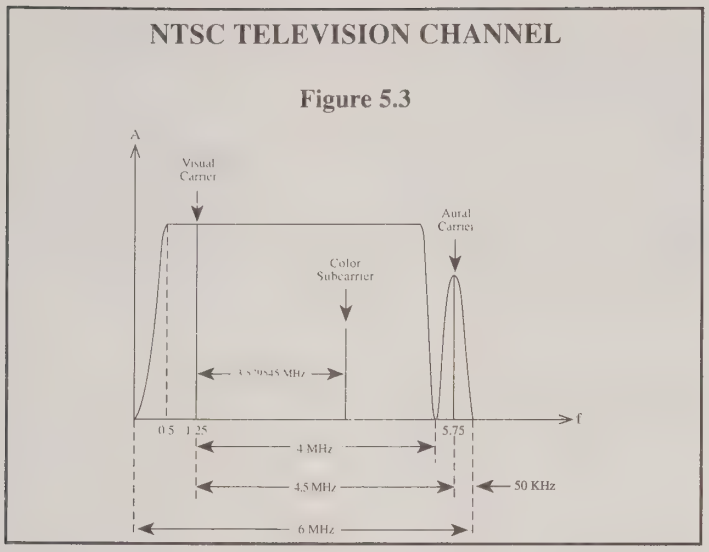
Figure 5.1

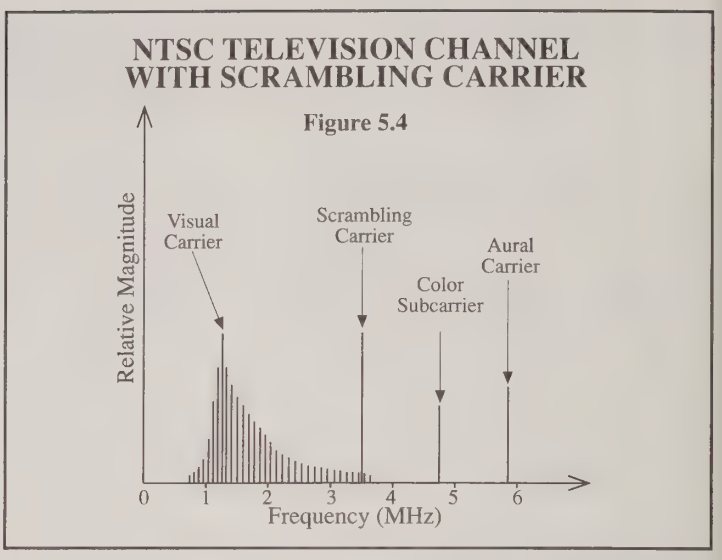


POSITIVE SECURITY SCRAMBLER

Figure 5.2







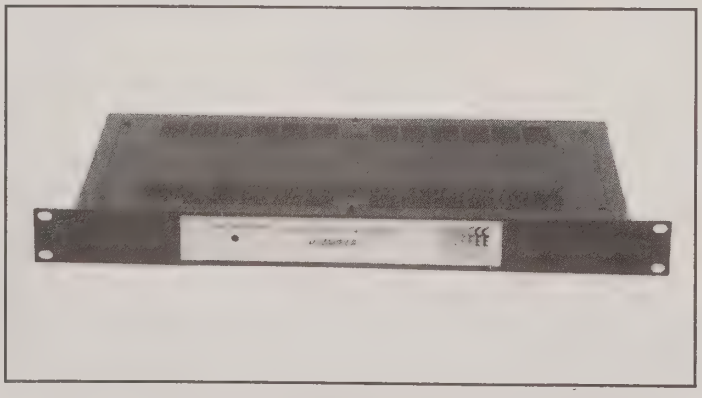
The frequency of the 2.257 MHz was carefully chosen to interleave between harmonics of the television scanning frequency without interfering with the chroma information carried by the color subcarrier. Beats and harmonics of the difference between the scrambling carrier frequency and the visual carrier frequency will become part of the 4.5 MHz aural carrier. These beats and harmonics will pass through the receiver's limiter and be demodulated as a 1.0 KHz tone which over-rides the audio. The 1.0 KHz signal also creates horizontal modulation bars in the picture.

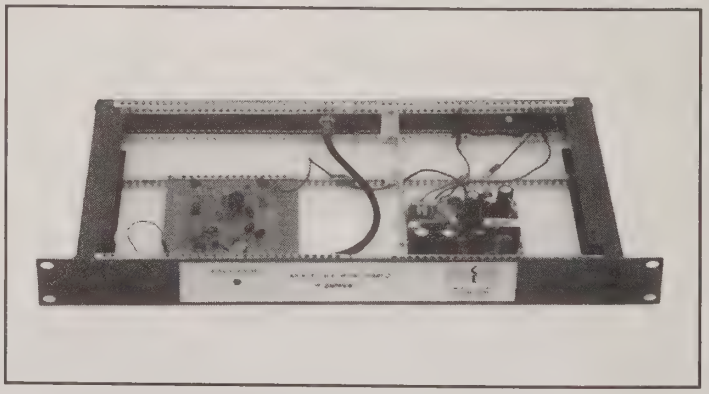
The 15 Hz signal interferes with both the receiver's *automatic gain control* (AGC) and the information in the color sub-carrier. It also interferes with the receiver's vertical synchronization pulses causing the picture to jump and roll and it creates a "chirping" noise in the receiver's audio.

At the subscriber's drop-line the jamming carrier is notched out using a trap tuned to the frequency of the jamming carrier. The notch has a 3 dB bandwidth of 1.25 MHz. Because the filter cannot distinguish between the desired visual carrier and the un-desired jamming carrier, the notch necessarily removes part of the visual carrier. Thus, the TEST system necessarily damages some of the visual signals. However, by tuning the jamming carrier to a frequency at the edge of the visual carrier's vestigial sideband spectrum and by keeping the jamming carrier relatively narrow, video damage is minimized. The reason can be understood when one looks at the amount of information in various parts of the video spectrum.

When a visual carrier is modulated, the video modulation produces sidebands. The density of these sidebands declines as one moves further away from the visual carrier frequency as shown in Figure 5.5. For channels below VHF Channel 6, the amount of information lost in a narrow notch filter is relatively small in relation to the total amount of information contained in all of the sidebands. Thus, picture degradation is minimized.

With conventional positive traps, as channel frequency increases the relative amount of video

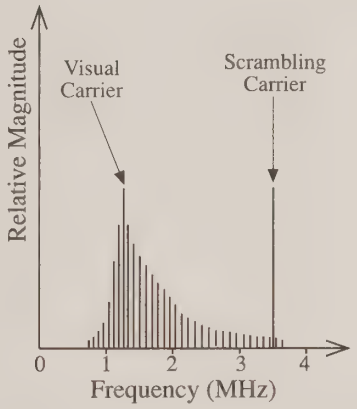




A typical modulator for a positive security system (Photo by C & E Corp.)

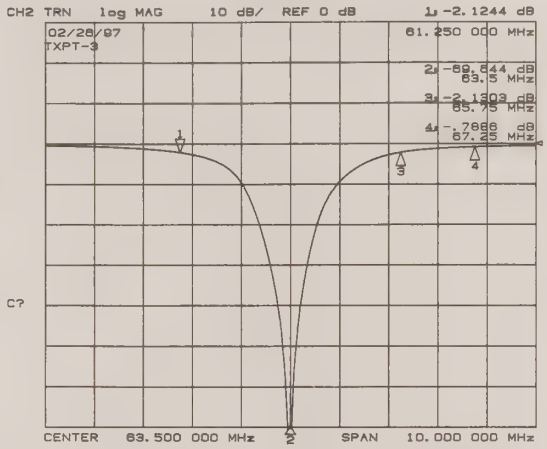
VESTIGIAL SIDEBAND INFORMATION

Figure 5.5



TYPICAL POSITIVE TRAP RESPONSE

Figure 5.6



information lost in the filter increases. This occurs because the bandwidth of notches increases with notch frequency. Above Channel 6, pictures will *begin* to "wash out" or lack definition and detail. At frequencies above Channel 13 this effect becomes so pronounced that pictures *eventually* become completely unusable. Thus, for NTSC Channels the TEST system is usually limited to frequencies below VHF Channel 13.

In order to further minimize the amount of degradation caused by positive traps, the headend scrambler *pre-emphasizes* the visual carrier by 15 dB in the region around the interfering carrier. This has the effect of narrowing the information lost in the notch to only 0.75 MHz. A phase-locked-loop (PLL) in the scrambler insures that the difference between the visual carrier and the scrambling carrier remains the same.

Other Discrete Jamming Systems. A number of other discrete jamming systems have been developed. *Arcom and Eagle* have developed two systems which are similar to the TEST System. The first is an RF system which uses two modulation signals, at 1.5 KHz and 10 Hz, instead of carriers at 1.0 KHz and 15 Hz. The second system does essentially the same thing but the carriers are inserted at *intermediate frequency* instead of RF. The discrete IF jamming system also incorporates a pre-emphasis circuit to improve video quality at high frequencies.

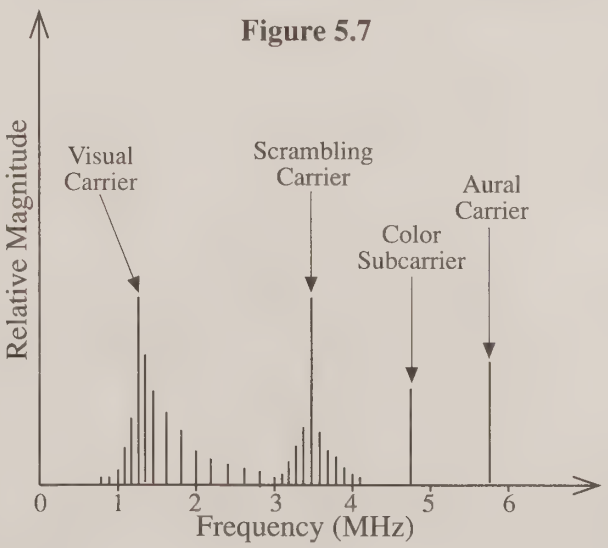
Pre-Emphasis Systems

A number of variations of the TEST system have been developed which use the principles of pre-emphasis and de-emphasis. Pre-emphasis has long been used in mobile FM radio as a means of improving audio quality at high frequencies. Because the insertion loss of circuits increases with frequency, higher frequency signals tend to be attenuated more than lower frequency signals. On cable television systems this effect is called "line-tilt." It results in amplitude distortion.

One way of rectifying amplitude distortion at higher frequencies is to pass the audio through a *pre-emphasis network*. The pre-emphasis network "emphasizes" or amplifies higher frequency signals more than lower frequency signals. A de-emphasis network does the reverse. Thus, de-emphasis

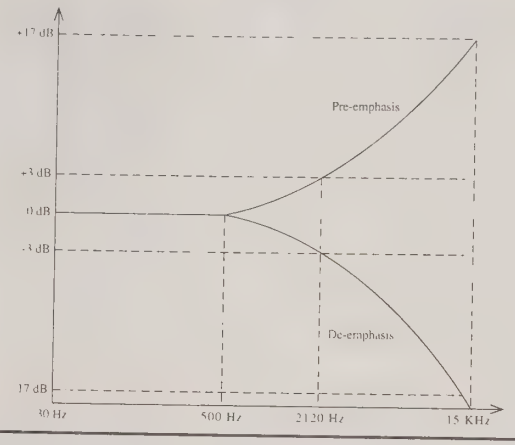
PRE-EMPHASIZED VIDEO WITH SCRAMBLING CARRIER

Figure 5.7



PRE-EMPHASIS & DE-EMPHASIS FOR FM MOBILE RADIO

Figure 5.8



networks are used in mobile FM receivers to "equalize" signals back to their proper relationships.

A certain amount of pre-emphasis is frequently used in positive security systems for enhancing the video signal in the region around the jamming carrier. This minimizes the damage which filters do to the video signal. However, the principles of pre-emphasis and de-emphasis have also been adopted by filter manufacturers to distort video amplitude and phase relationships. Both the *Sideband Interdiction System* and the *Gaussian Security System* make use of pre-emphasis and de-emphasis.

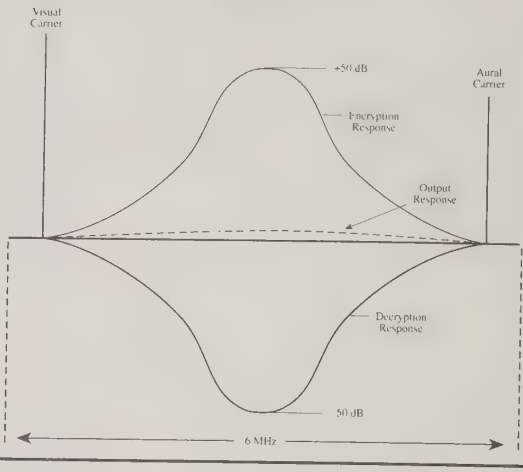
Sideband Interdiction

The "*Sideband Interdiction System*" (SIS) has been patented by *Eagle Comtronics Inc.*[4] Unlike the TEST system, SIS does not use an interfering carrier to "jam" the visual carrier. Instead, SIS works by *pre-emphasizing* the video response at the headend by 50 dB. A pre-emphasis network is used to exaggerate video levels in the region where the jamming carrier is normally inserted. Thus, the video carrier's own energy is used to scramble the channel. However, unlike the semi-linear responses used with FM transceivers, the pre-emphasis response used in SIS is shaped like a bell.

Signals are de-emphasized using a positive filter in the subscriber's drop-line. The response of the positive filter acts as a de-emphasis network. The shape of the de-emphasis response is an "inverse" or "mirror image" of the pre-emphasis response used at the headend. Thus, SIS is not a real "jamming" system. Since SIS actually *modifies* or *transposes*

EAGLE'S SIDEBAND INTERDICTION SYSTEM

Figure 5.9



video signals of fixed duration, the system classifies as a cipher system.[5] Cryptographers would call it a "scrambling" system. The frequency response of the *pre-emphasis network* is the *encryption algorithm.* The frequency response of the *de-emphasis network* is the *decryption algorithm.*

Because the filters used in SIS function to reverse distorted signal levels introduced at the headend, video signals are never "lost" in the filtering process. Thus, the resulting video quality is superior to that of the original TEST system. Because no video signals are actually "cut out" of the video sideband, SIS may be used on channels up to 450 MHz. However, for technical reasons SIS cannot be used on *amplitude modulated microwave links* (AMLs) without special modifications.

Because the drop-line filter used to de-emphasize the video must have a frequency response which is the inverse of the pre-emphasis response, video

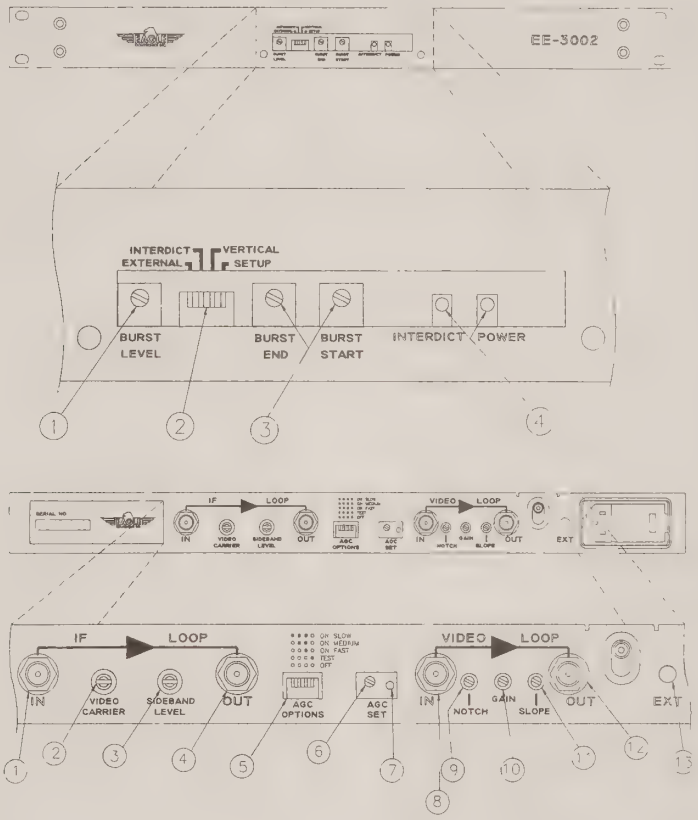
[4]Patent No. 5,148,133.

[5]It is common for filter manufacturers to refer to their modulators as "encoders" and positive traps as "decoding filters." Since the TEST security system does not *really* use "codes," the terminology is *technically* incorrect. Since *SIS* and the *Gaussian System* transform the amplitude and phase of signals which have a fixed duration, the respective filters would be more correctly described as "de-ciphering" filters. Although the TEST system uses some pre-emphasis, it is not used as a ciphering system. The pre-emphasis used in the TEST system is primarily intended to improve video quality. Cf. Gaines, p. 1; Kahan, p. xv, Lysing, p. 1; Smith, p. 16; Polmar and Allen, pp. 122, 127; and the ***American Heritage Dictionary of the English Language.*** pp. 274, 278.

FRONT & BACK PANEL OF SIS SCRAMBLER

(Courtesy of Eagle Comptronics)

Figure 5.10



quality will not be restored using just "any old notch filter" with a specific depth and stopband width. The filter *must* have a response which is a "mirror image" of the pre-emphasis response used at the headend. Thus, "pirate" filters are more difficult to fabricate.

The Gaussian System

The "*Gaussian Positive Security System*"[6] was developed by *Arcom Labs*. Video is passed through a pre-emphasis network which emphasizes the central region of the video band by 30 dB. The frequency response of the pre-emphasis network follows a "Gaussian" curve. Students of statistics will recognize a "Gaussian" or "Laplacian" curve as a "normal distribution" given by the function:

[1] $y = [1 / \sigma (2\pi)^{1/2}] \exp. [(-1/2) (x^2 / \sigma)]$,where:

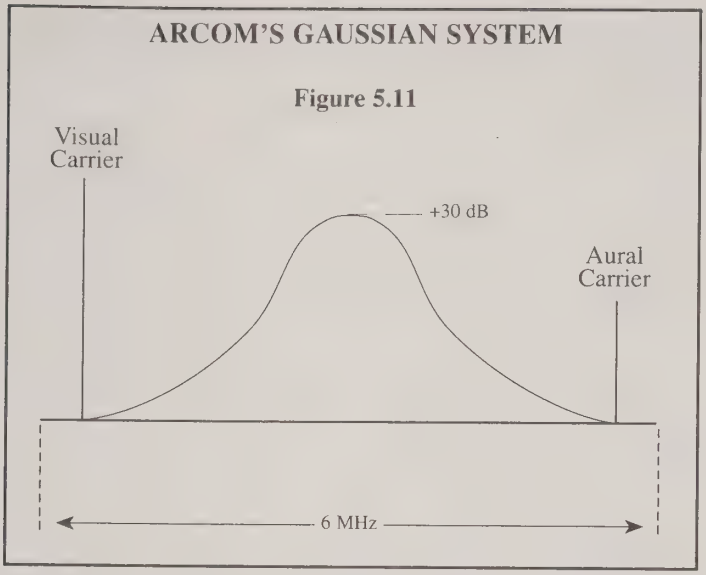
σ =the standard deviation of the curve,
y = the vertical axis value, and
x = the horizontal axis value.

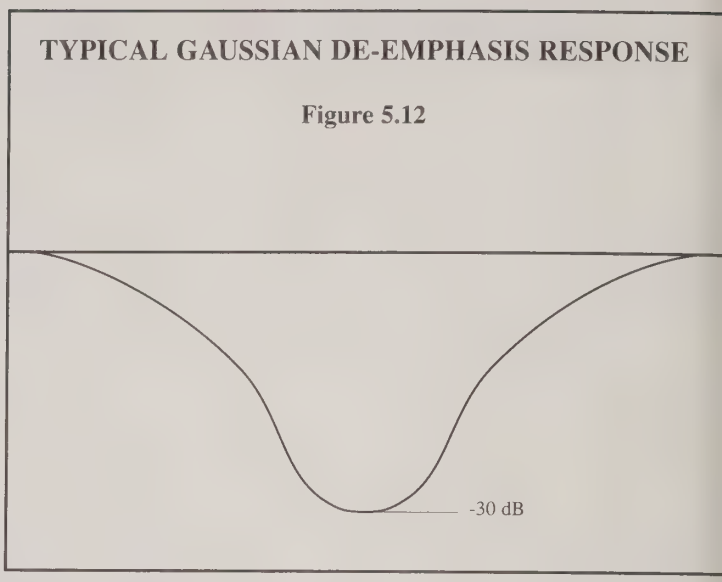
Thus, the Gaussian function has *a whole family of curves* for various values of "σ."

A gated jamming carrier is inserted in the channel at 2.25 MHz above the visual carrier. The gated carrier is turned on *only during the horizontal and vertical blanking intervals.* This reduces distortion introduced by the jamming carrier.

Once jamming signals are added to a waveform there are only two ways of removing them - (1) phase cancellation or (2) filtering. Whenever two signals are added in a non-linear device, they tend to "beat" or heterodyne together. This produces *sum and difference* frequencies. Thus, although shutting off the jamming carrier during the video scanning period does *not* reduce the amount of intelligence removed during filtering, it does reduce the amount of distortion introduced during the scanning period. Because the jamming carrier is only present during the blanking intervals, it tends to leave the video

[6] Patent No. 34,720





signal unharmed while disrupting the synchronization of the receiver. Because the receiver is relatively insensitive to distortion during the vertical and horizontal blanking intervals, the additional distortion is ignored by the receiver circuits.

The positive trap used in the subscriber's drop-line contains a notch for filtering the jamming carrier and a de-emphasis network for de-emphasizing the video signal. The primary purpose of the Gaussian pre-emphasis network is to improve picture quality by enhancing the video signals in the spectrum around the jamming carrier.

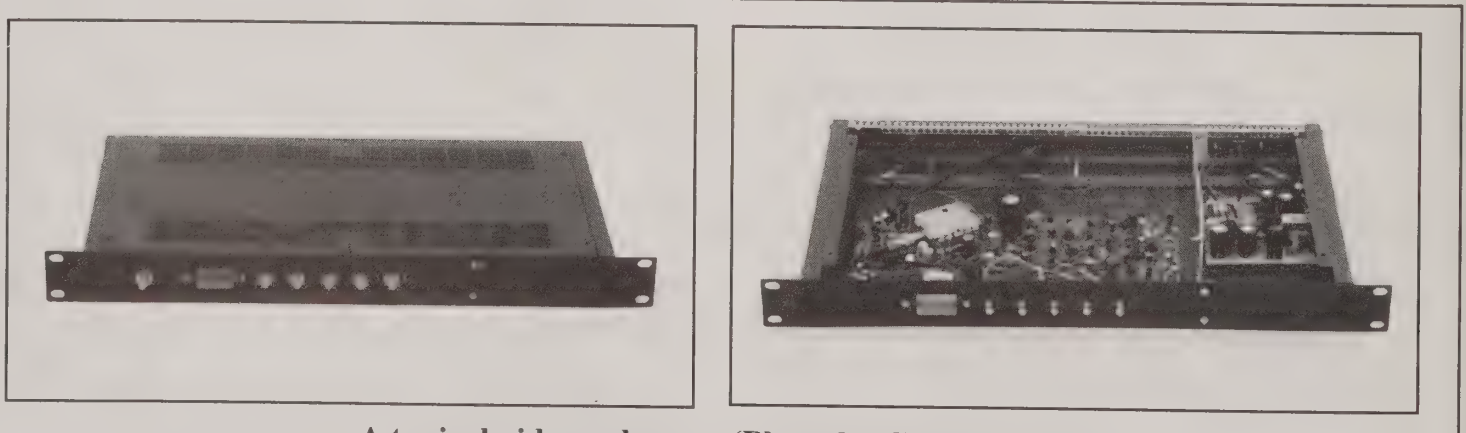
The Gaussian system has three security ramifications. First, if a simple notch filter - without a de-emphasis network - is placed in the drop-line, the pirate may see a degraded picture but would not want to watch it. Second, a pirate attempting to fabricate or design a positive trap for recovering the video would need to know how to design a Gaussian de-emphasis network. Third, the pirate would have to find the exact curve used by *Arcom* in the pre-emphasis network.

The SAWDEC System

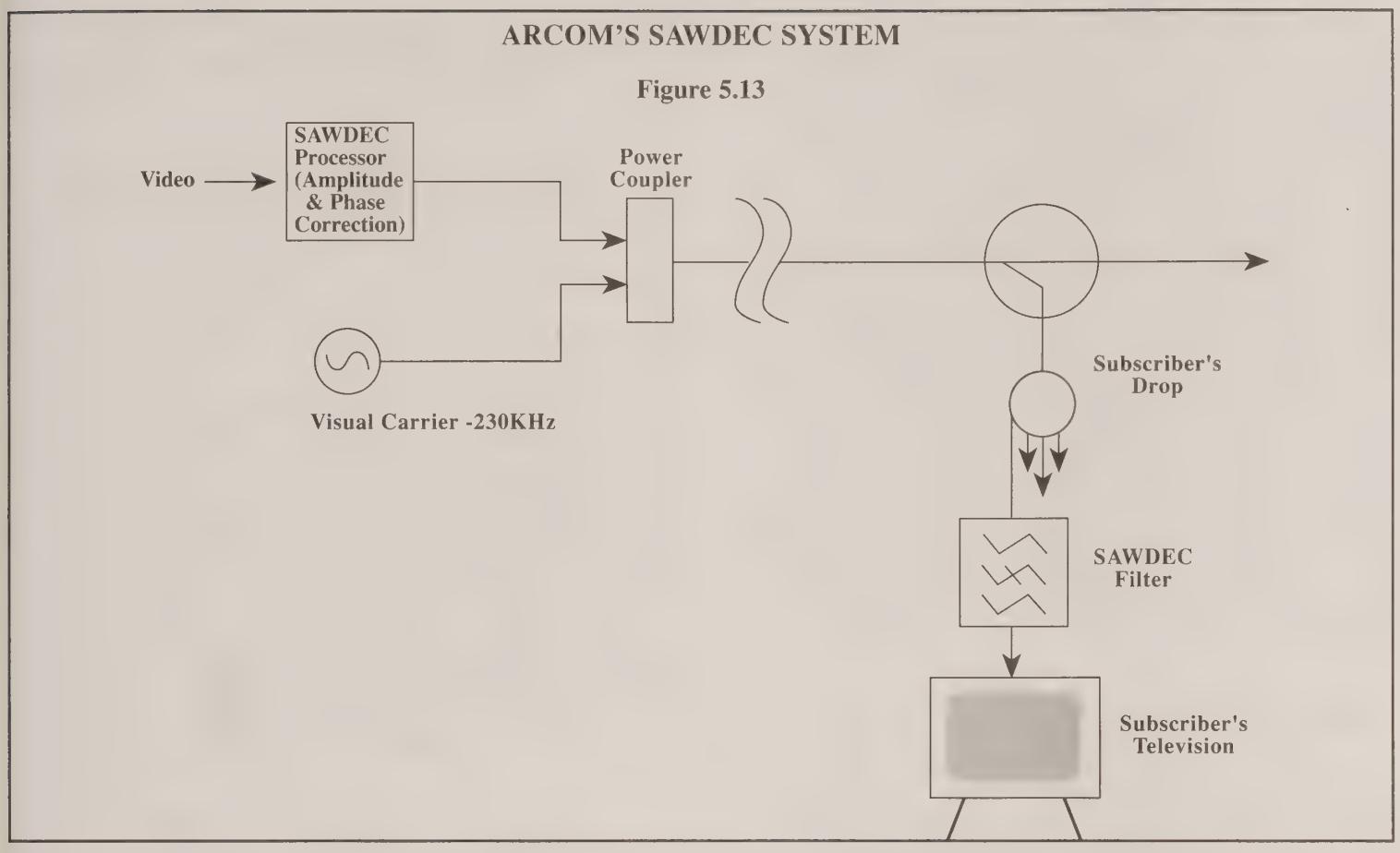
Arcom Laboratories recently completed development of a new positive scrambling system (Patent Pending) called *"SAWDEC."* The present system can be used at frequencies of up to 450 MHz. The *SAWDEC* system is similar to conventional positive security systems in that signals are *enciphered* at the headend and *deciphered* at the subscriber's drop-line using a passive filter. However, *SAWDEC* differs from traditional systems in several significant ways. In fact, the differences are truly *"revolutionary."*

First, unlike conventional systems the *SAWDEC* encryption system uses a jamming signal at 230 KHz *below* the visual carrier. Since the jamming carrier is so close to the visual carrier, an *extremely high Q filter is required* to remove it without removing the visual carrier itself.

Second, unlike traditional systems *SAWDEC* makes use of an extremely narrow *Surface Acoustical Wave*



A typical video enhancer (Photo by C&E Corp.)

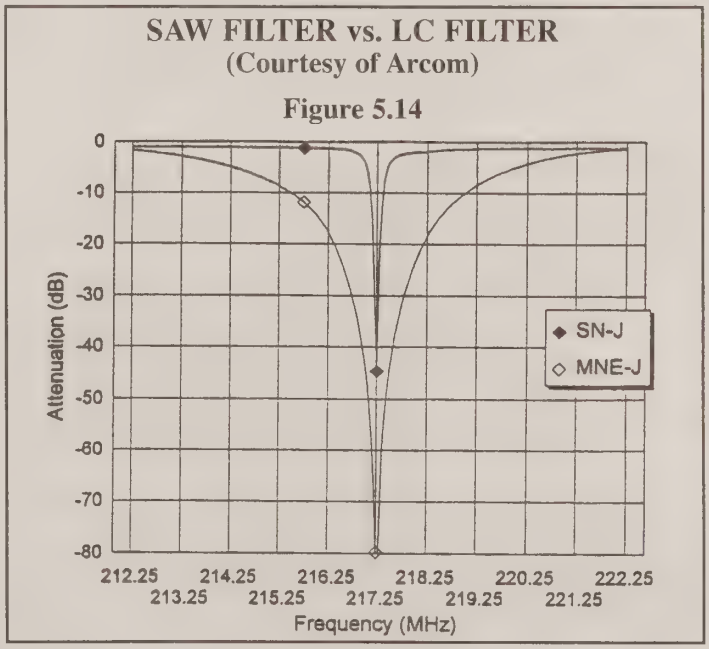


(SAW) filter in the subscriber's drop-line. Because SAW filters can be made with extremely narrow bandwidths, *SAWDEC* filters can effectively remove a jamming carrier near the visual carrier without removing the visual carrier itself. Hence, when combined with amplitude and phase correction at the headend processor, the amount of video removed from the channel by the *SAW* filter can be reduced to levels far below those of conventional L-C filters constructed using discrete components. Because *SAW* filters are *not affected* by humidity and because they are very *temperature stable*, use of highly selective notches close to the visual carrier is practical.

Third, unlike conventional systems, the headend encryption unit changes both the *phase and the amplitude* of the video frame by frame using a state-of-the-art *digital compensation processor*. Each video frame is digitally stored and processed using a twenty bit word. The processor compensates the video using a ninth order FIR filter to calculate the required phase and amplitude correction.

For several reasons, *SAWDEC* video quality is far superior to conventional positive security systems. The combination of a highly selective *SAW* filter with amplitude and phase correction at the headend results in an *extremely narrow equivalent notch*. Given a fixed notch depth, SAW filters are capable of reducing bandwidths to one tenth the widths of LC filters. This minimizes the amount of signal removed from the channel and maximizes quality. Because the television receiver does not really use the vestigial sideband on the opposite side of the visual carrier to make a picture, signals removed from the vestigial sideband are still present in the other sideband.

Because only a SAW filter tuned to the correct



frequency can achieve a notch sufficiently selectively to remove only the jamming carrier, SAWDEC is more secure than conventional positive security systems. Homemade filters constructed using discrete components simply cannot be substituted. Finally, since the production of SAW filters requires a considerable capital investment in addition to technological know-how, production of pirate filters in small quantities is financially prohibitive. Further, anyone duplicating a *SAWDEC* filter would have to duplicate the filter's exact frequency and phase response. Unauthorized production of Patented *SAWDEC* filters would violate *Arcom's Patent* in addition to a variety of state and federal piracy laws. Hence, civil action by both *Arcom* and the injured cable operator would be possible.

Positive Filters

In general, filters for positive security systems may be classified as either - (1) patented security filters, or (2) discrete system filters. Positive security filters may be mounted either in the subscriber's drop-line at the tap or inside a set-top converter box. Tap mounting makes the filters less accessible to the subscriber but the trap is exposed to harsher conditions. It also exposes the trap to anyone who might climb the pole to break it off the tap. Mounting filters inside the set-top converter stabilizes the temperature, limits exposure, and reduces installation costs. However, the filter is much more accessible to anyone who has access to the subscriber's home. If the filter is lost or stolen, anyone who has the filter can recover the program anywhere on the cable system. Thus, each mounting location has its advantages and disadvantages.

Patented Security Systems. The Sideband Security System, the Gaussian system, and the SAWDEC system are under patent. All use *non-generic* pre-emphasis and de-emphasis networks. *Eagle Comtronics* also uses some pre-emphasis in its *Discrete IF System* to improve video quality at higher frequencies.[7] Visual carriers are pre-emphasized by 3.0 dB while aural carriers are pre-emphasized by 5.0 dB. A pre-emphasis of 30 dB is used at the jamming carrier frequency.

Discrete Security System Filters. Discrete security methods based upon the TEST system use fairly generic notches to filter out jamming carriers. Since positive notches are used at frequencies between the visual carrier and the color subcarrier, the notches must minimize the level of insertion loss on the channel's visual and aural carrier. Although specifications vary from one manufacturer to another, positive traps generally have notches of 70 or 80 dB with passbands up to 1 GHz. Passband insertion losses usually range between 1.0 dB (on lower channels) and 2.5 dB (at 1 GHz). Video losses typically range 1.4 dB (on lower channels) and 6.0 dB (on Channel 13).

[7]Filters for Eagle's discrete IF jamming system are currently under patent. Cf. Patent Nos. 4,451,803; 5,148,133; and 5,168,251.

Works Consulted

---------- , ***American Heritage Dictionary of the English Language.*** 2nd Edition. Boston: Houghton Mifflin Company, 1982.

Arcom CATV Products, "MP Series Double Density Positive Traps" [Informational Monogram]. Syracuse, New York: Arcom CATV Products, nd., pp. 1-3.

Eagle Comtronics, Inc., "Application Notes: Sideband Interdiction System EE-3000" [Technical Monogram; AN903002 Rev. 0]. Clay, New York: Eagle Comtronics, Inc., 1995.

Eagle Comtronics, Inc., "Decoding Filters SIS" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "EE2002, EE3002, and EOSC Encodes for Positive Filters" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "How Positive Filters Work" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "Micro Series Decoding Filters" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Eagle Comtronics, Inc., "Ultra Narrow Decoding Filters" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Helen Fouche Gaines, ***Cryptanalysis: A Study of Ciphers and Their Solution.*** New York, N.Y.: Dover Publications, 1939.

Brent Gale and Frank Baylin, ***Satellite and Cable TV Scrambling and Descrambling***. Second Edition. Boulder, Colorado: Baylin/ Gale Productions, 1986.

International Telephone and Telegraph. ***Reference Book for Radio Engineers.*** New York: Howard W. Sams & Company, Inc. 1991.

David Kahn, ***The Codebreakers: The Story of Secret Writing.*** New York, N.Y.: Macmillan Company, 1967.

Henry Lysing, ***Secret Writing: An Introduction to Cryptograms, Codes, and Ciphers.*** New York, N.Y.: Dover Publications, 1974.

Pico Products, Inc., "Collected Filter Specifications & Spectrum Plots" [Loose leaf collection of photocopied spectrum plots and product information provided by manufacturers representative]. Liverpool, New York: Pico Products, Inc., nd [1994].

Norman Polmar and Thomas B. Allen, ***Spybook: The Encyclopedia of Espionage.*** New York: Random House, 1977.

Lawrence Dwight Smith, ***Cryptography: the Science of Secret Writing.*** New York, N.Y.: Dover Publications, 1971.

James Tanner, "United States Patent: Television Security System: Patent No. 4,074,311 dated February 14, 1978." Washington, D.C.: U.S. Department of Commerce Office of Patents and Trade Marks, 1978.

Chapter 6
The Economics of Filtering

After cable television was introduced in the United States, CATV systems became regulated monopolies. Today, the situation is rapidly changing. Deregulation and a variety of market forces have placed increasing pressure on cable operators to keep costs low. Cable operators face *increased competition* from a number of *alternative delivery systems.* Competition from services like *Blockbuster Video*, *Direct Broadcast Service* (DBS), multi-channel wireless (MDS/MMDS) television systems, multi-channel *Low Power Television* (LPTV) systems, and digital broadcast television has created increased competition in the market place.

Currently a multi-channel wireless system can be launched for around half the expense of building a conventional coaxial cable system. Fiber optical systems are even more costly than coaxial systems. Unlike conventional cable systems, wireless installation expenses grow proportionally with revenue. With CATV systems an operator must wire a *whole franchise area* regardless of penetration. With the introduction of *digital channel compression*, the number of channels which wireless systems can offer will expand from a maximum of thirty-three analog channels to somewhere between sixty-six and three hundred-thirty digitally compressed programs. As the number of DBS subscribers increases, the cost of DBS equipment will decline making it more economical for subscribers to install DBS reception systems. Digital broadcast systems and digital channel compression will allow high power television broadcasters to transmit either two *high-definition television* (HDTV) programs or between four and twenty low-resolution programs using only two 6 MHz broadcast channels. A number of twenty channel analog LPTV systems are already operational both in the United States and abroad. Digital channel compression could expand such analog channel capacity by a factor of ten.

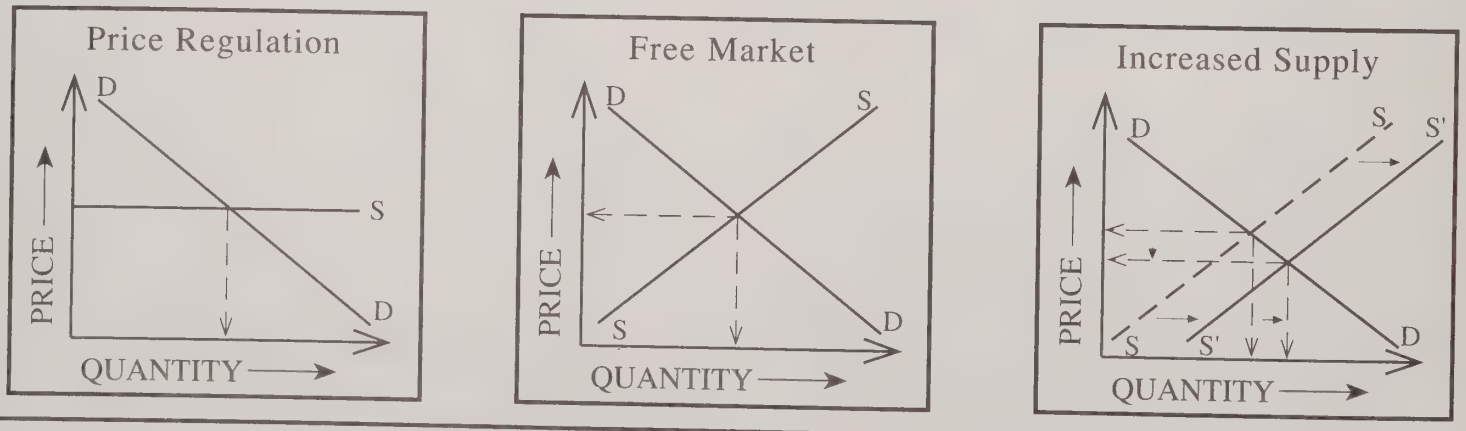
There is a limit to how many channels a person can watch during a finite period of time. For example, DBS may provide five hundred digitally compressed channels but it would take 8.33-hours for a subscriber to watch only one minute of each channel. Beyond a certain "saturation point" the larger channel capacity of fiber cable systems will not give those systems a *decisive* programming advantage over emerging technologies. Increased variety does not necessarily translate into increased sales.

All of these macro-economic developments have radically altered the economics of the cable business. Figure 6.1 illustrates the differences using simplified economic models. Increased competition places downward pressure on prices.

In the future the profitability of CATV systems will depend increasingly upon the ability of cable operators to keep costs low.

SIMPLIFIED ECONOMIC MODELS

Figure 6.1



SCENARIO ONE*

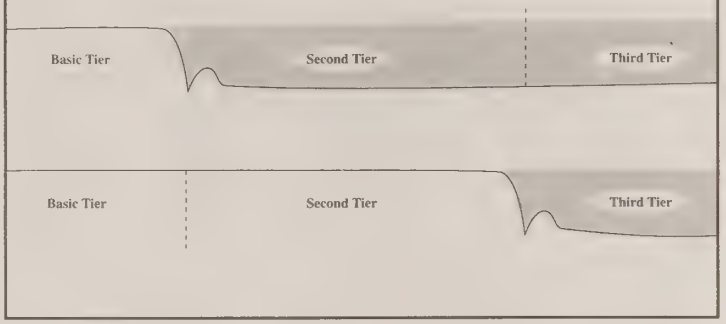
Table 6.1

Basic Customers:	**15,000**
Second Tier Customers:	**10,000**
Third Tier Customers:	**5,000**
Total:	**30,000**

***Upper tier customers are assumed to subscribe to all lower tiers.**

LOWPASS TIER FILTERING

Figure 6.2



Pay television filtering has survived because it is *effective* and *inexpensive.* Positive trapping is frequently one of the least expensive methods of securing programming. Negative filtering is one of the most secure methods. In many cases negative filtering can be equally inexpensive. In order to fully exploit the *financial advantages of filtering*, it is necessary to understand its financial dynamics. This makes it possible to apply filtering in the most economical ways possible in order to maximize profits. It is possible to explore these dynamics using a series of increasingly sophisticated hypothetical models.

Tier Filtering vs. Set-Tops Converters

During the early days of cable television it was necessary to equip customers with set-top converters because standard television sets were limited to the VHF lowband and VHF highband. Under those circumstances it was relatively easy to incorporate a variety of security devices into the set-tops. In fact, some operators used to place their positive traps inside the converters.

Cable compatible television sets eliminated the need for set-tops which served merely as tuners. So, today set-top converters are only cryptographic security devices. They typically cost between $ 50.00 and $ 300.00 depending upon the sophistication of the particular unit. The least expensive *generic units* consist of a mass produced "channel tuner" in a box. The most expensive units are complex digital set-tops with sophisticated encryption circuits. To compensate for the loss of television features involved in using an *external converter*, some set-top converters incorporate a variety of features usually found on television sets. Typical features include "on-screen programming," remote control, timers, and a variety of other options. However, more features just pushes up costs for both the cable operator and the subscriber while unnecessarily duplicating features already on the subscriber's television.

Case 1. If we assume a cable system with the penetration rates illustrated in *Scenario One* (Table 6.1), we can compare the cost of set-top converters with the cost of tier filtering. To keep the estimates *"conservative,"* the price of a set-top will be estimated at only $ 75.00 per unit. With 30,000 subscribers the total cost of set-top converters would be:

[1] 30,000 x $ 75.00 = $ 2,250,000.00

To secure the first (basic) and second tiers using negative filters would require 25,000 negative filters. The operator would need 15,000 lowpass filters for the first tier and 10,000 negative lowpass filters for the second tier. A relatively simple lowpass filter could be used on each tier. Tubular filters typically cost between $ 5.00 and $ 20.00 depending upon the quantity purchased. However, to keep our estimates *conservative*, we could assume the higher estimate of $ 20.00 per filter. Thus:

[2] 25,000 x $ 20.00 = $ 500,000.00

[3] / ∴ $ 500,000.00 < $ 2,250,,000.00

Clearly, *under these circumstances* using filters would save $ 1.75-million over equipping all subscribers with set-top converters. *It is for exactly this reason that few cable operators still equip basic or second*

SCENARIO TWO*

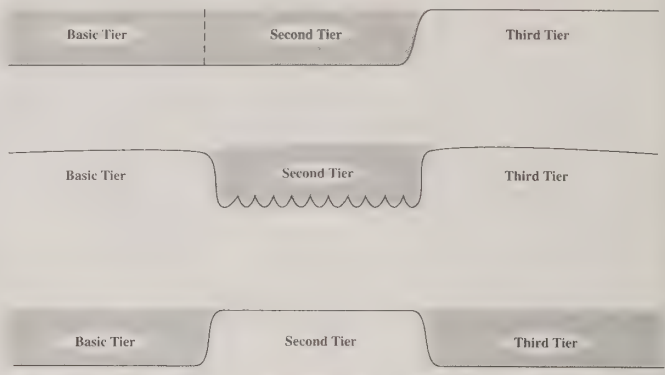
Table 6.2

Basic Customers	**10,000**
Second Tier Customers	**15,000**
Third Tier Customers:	**5,000**
Total:	**30,000**

***Upper tier customers are assumed to subscribe to all lower tiers.**

BSF, BPF, & HPF TIER FILTERS

Figure 6.3



tier customers with set-top converters.

Filtering & Set-Top Converters

Set-top converters do have some advantages over filtering. They allow the operator to use PPV and IPPV services. In addition, set-tops encipher more individual premium movie channels than can be secured using single channel traps. However, because set-tops with good encryption systems are costly, it is desirable *to limit their use to only those applications where revenue justifies the expense.*

Some operators use a combination of filtering with set-top converters to *get the best of both worlds.* If channels are properly arranged, this approach has certain security advantages. It is possible to arrange the tiers in a cable system so that the security provided by filters adds to the security provided by the set-top converters. For example, if all premium movie channels are placed on upper tiers and negative tier filters are used on lower tiers, then set-top converters could be given to only upper tier customers who subscribe to one or more premium movie channels. Hence, a pirate converter box or even the operator's own authorized converter *will not work on lower tier drop-lines because the tier filters stop upper tier signals at the tap.*

We can explore a number of hypothetical financial scenarios using the same methods applied above. Cases 2, 3, and 4 are based upon *Scenario Two* shown in Table 6.2.

Case 2. If the cable operator equipped only second and third tier customers with set-tops and used tier filters for basic customers, the operator would need 20,000 set-top converter at $ 75.00 each and 10,000 filters at $ 20.00 each. The tier filter could be a simple lowpass filter which cuts off between the basic tier and the second tier. It follows that:

[4] 20,000 x $ 75.00 = $ 1,500,000.00

[5] 10,000 x $ 20.00 = $ 200,000.00

[6] $ 200,000.00 + 1,500,000.00 = $ 1,700,000.00

[7] / ∴ $ 1,700,000.00 < $ 2,250,000.00

Under these circumstances, using filters on the basic tier would save the operator $ 550,000.00.

Case 3. Suppose an operator equipped only third customers with set-top converters and used tier filters on the first and second tiers. It follows that the operator would require 5,000 set-tops and 25,000 tier filters. Thus:

[8] 5,000 x $ 75.00 = $ 375,000.00

[9] 25,000 x $ 20.00 = $ 500,000.00

[11] $ 375,000.00 + $ 500,000.00 = $ 875,000.00

[12] / ∴ $ 875,000.00 < $ 2,250,000.00

[13] / ∴ $ 875,000.00 < $ 1,700,000.00

Under the circumstances filtering could save the operator $ 1.375-million, over equipping all customers with set-tops, and $ 825,000 over

equipping both second and third tier customers with set-tops. Since basic customers would require only one negative lowpass filter and second tier customer would require a different lowpass filter, only one filter would be needed per tap.

Table 6.3 shows the costs of four different subscription scenarios. Case A illustrates a minority of basic tier customers and a majority of third tier customers while Case D illustrates the opposite situation. Cases B and C illustrate minorities and majorities in the second tier. It should be evident that the total cost of set-tops is proportional to the number of third customers. Hence, revenue grows with set-top expenses.

SUBSCRIPTION SCENARIOS*

Table 6.3

- (a) Subscribers -

	Case A	Case B	Case C	Case D
Basic	5,000	10,000	5,000	15,000
2nd Tier	10,000	5,000	15,000	10,000
3nd Tier	15,000	15,000	10,000	5,000
Total:	30,000	30,000	30,000	30,000

- (b) Costs -

	Case A	Case B	Case C	Case D
Filters:	$ 300,000	$ 300,000	$ 400,000	$ 500,000
Set-Tops	$ 1,125,000	$ 1,125,000	$ 750,000	$ 375,000
Total:	$ 1,425,000	$ 1,425,000	$ 1,150,000	$ 875,000

*Set Top Converters are used on the third tier.

Case 4. The Case 3 scenario presumed that all third tier channels are enciphered. Under that presumption all third tier customers must be equipped with set-tops to decipher third tier channels. However, actually this is unnecessary because third tier channels are already protected by the tier filters used on basic and second tier taps. *Thus, additional savings could be realized by enciphering only individual premium movie channels along with PPV and IPPV channels.* Under this plan subscribers who receive low cost commercial satellite channels on the third tier would not require set-tops.

If we assume that half the customers on the third tier want at least one premium channel, set-top converter expenses would be:

[14] 2,500 x $ 75.00 = $ 187,500.00

The total cost of lowpass filters would be:

[15] 25,000 x $ 20.00 = $ 500,000.00

Hence the cost of tier filters and set-tops would be:

[16] $ 187,500.00 + $ 500,000.00 = $ 687,500.00

[17] / ∴ $ 687,500.00 < $ 2,250,000.00

[18] / ∴ $ 687,500.00 < $ 875,000.00

Therefore, the operator would save $ 1.5625-million over equipping all customers with set-tops and $ 187,500 over equipping all third tier customers with set-tops.

Thus far we have assumed that lowpass filters are used as tier filters. Hence, if the operator used only lowpass pay filters, it would be necessary to subscribe to the first and second tiers in order to get the third tier.

Wide bandstop filters and wide bandpass filters make it possible for the cable operator to provide individual tiers one at a time. For example, if a wide bandstop filter tuned to block only the second tier is placed in a subscriber's drop-line, the subscriber will receive only the first and third tiers. Similarly, using a bandpass filter tuned to the second tier, the operator could provide customers with only second tier channels. Likewise, using a highpass filter, the operator could provide only the third tier by blocking the first and second tiers.

Obviously many variations of Case 4 are possible. For example, using lowpass filters, an operator could continue to divide up the remainder of the CATV band into more tiers. Alternatively, an operator could use the encryption capability of the set-top to establish a *fourth tier.* Thus, set-top converters would be given only to customers who subscriber to individual premium channels on the third or fourth tiers.

Analyzing Costs. If no one on the cable system subscribed to pay services, the operator would need a

negative tier filter for all subscribers to secure premium channels. If there were no premium customers and the operator equipped only premium customers with set-top converters, the operator would not have to buy any set-top converters at all. Thus, under certain circumstances, set-top converters may be less expensive than tier filters. Assuming the costs used previously, Table 6.4 shows that set-top converters are less expensive than tier filters when penetration rates are somewhere between 12.5-percent and 25-percent.

It is possible to calculate *the exact point* at which using tier filters costs the same as using set-tops. So far we have assumed that tier filters cost $ 20.00 each and that set-tops cost $ 75.00 each. Since *this may not always be the case*, operators need a general formula for calculating costs.

In general, given a specific population of subscribers, the exact point where using set-tops costs the same as using tier filters can be determined by solving *two linear equations in two variables.* The cost of negative tier filtering may be calculated using the equation:

[19] $y = C_t (n - x)$, where:

y = the total cost of tier filtering ($),
x = the number of premium customers,
C_t = the price per negative tier filter ($), and
n = the total number of subscribers on the system.

The cost of using set-top converters may be calculated using the equation:

[20] $y = C_s x$, where:

y = the total cost of using set-tops ($),
x = the number of premium subscribers, and
C_s = the price per set-top converter ($).

Equations [19] and [20] may be "solved" for "x" by setting the two equations equal to each other[1] and using some algebra:

[21] $y = C_t (n - x) = C_s x$.

TIER FILTERING vs. SET-TOP CONVERTERS*

Table 6.4

Premium Subscribers	Penetration (%)	Tier Filtering ($)	Set-Tops ($)
0	0.0	400,000	0
2500	12.5	350,000	187,500
5000	25.0	300,000	375,000
10,000	50.0	200,000	750,000
15,000	75.0	100,000	1.125-million
20,000	100.0	0	1.5-million

* The table assumes a total population of 20,000 subscribers with costs of $ 20.00 per filter and $ 75.00 per set-top converter.

For example, assuming the values used in previous calculations, we would have:

[22] $y = \$ 20.00 (20{,}000 - x) = \$ 75.00 x$
$400{,}000 - 20x = 75x$
$400{,}000 = 95x$
$95x = 400{,}000$
$x = 400{,}000 / 95$
$/ \therefore \quad x = 4210.5263$ subscribers

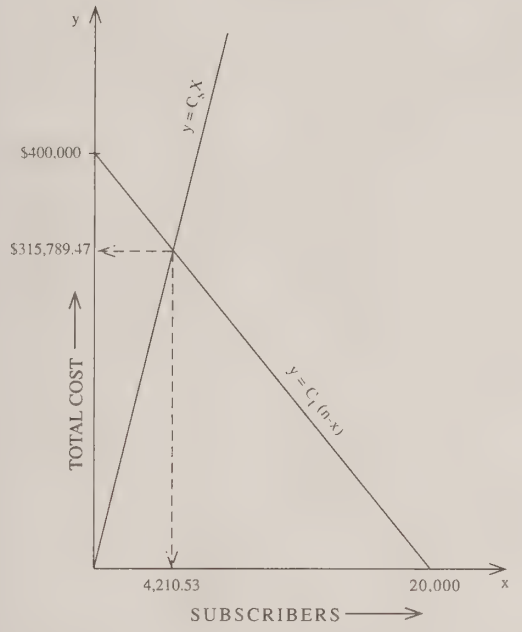
Figure 6.4 illustrates a graph of the two equations showing the point where the two equations intersect. Thus, with a subscriber population of 20,000 if filters cost $ 20.00 each and set-top cost $ 75.00 each, the total cost of set-tops will be equal to the total cost of tier filters when one has approximately 4211 premium subscribers. This corresponds to a penetration rate of around 21-percent. If the number of upper tier customers in the specific population *grows* above 4211 customers, then negative tier filtering would be cheaper.

Given a set-top converter at a particular price, the cost of the *individual premium channels* deciphered by set-tops declines as the number of premium channels increases. Table 6.5 illustrates this fact.

[1]There are a number of methods for solving systems of linear equations but this method should work for the kind of problems encountered with pay TV filters. For other methods cf. E.W. Swokowski, ***Fundamentals of Algebra and Trigonometry.*** pp. 367, 372, *passim.*

GRAPH OF COST EQUATIONS

Figure 6.4



Thus, if set-tops cost $ 75.00 each and single channel filters cost $ 20.00 each, the set-top converter has to carry four channels before it is less expensive than using filters. Although this number does not take converter maintenance costs into account, it may be used for making rough estimates.

In general, given the cost of a set-top and the cost of a particular channel trap, the number of channels needed for the costs to be equal may be calculated using the equation:

[23] $\mathbf{N_c = C_s / C_f}$, where:

N_c = the number of premium set-top channels for costs to be equal,
C_s = the cost of each set-top converter, and
C_f = the cost of each filter.

From the foregoing analysis we can conclude that set-top converters are most profitable with small high revenue populations which subscribe to a lot of higher price premium movie channels. *It is for exactly this reason that some cable operators are pulling set-top converters out of homes and using filters in their place.*

PREMIUM CHANNEL COSTS*
(Using Set-Top Converters)

Table 6.5

Number of Channels	Cost Per Channel
1	$ 75.00
2	$ 37.50
3	$ 25.00
4	$ 18.74
5	$ 15.00
6	$ 12.00
7	$ 10.71
8	$ 9.38
9	$ 7.50

*** The table assumes that set-top converters cost $ 75.00 each and that single channel filters cost $ 20.00 each.**

Single Channel Trapping

Certain older premium movie channels, like *HBO* or *Cinemax*, may be so popular in certain geographic areas that a large number of customers will subscribe if the channel is available individually. We have assumed that all premium movie channels are placed in upper tiers and deciphered using set-top converters. To get a single premium channel basic tier customers must purchase all of the channels on the third tier and rent a set-top converter.

Given the circumstances, a cable operator might want to make a popular movie channel available to *all subscribers on an individual basis.* This could be done by simply placing enciphered channels in the lower tiers and giving a set-top to all customers who want individual channels. However, if tier filtering is used in the system, then the subscriber would at least have to purchase the whole tier which contains the desired channel. Because the *rental costs* involved in providing set-tops adds to the subscriber's expense, the *additional costs* involved in taking only one channel may influence subscriber demand for the premium channel. For example, a subscriber who is willing to sign up for HBO at $ 12.00 per month may not want to take a whole channel tier at $ 10.00 and pay a set-top rental fee of $ 6.00 per month just to get HBO. Customers who will take HBO for an

SCENARIO THREE

Table 6.6

Premium Customers	**11,000**
Total Customers:	**20,000**

additional $ 12.00 per month, may not sign up if it ends up costing them an additional $ 28.00 per month.

Even if the customer is willing to pay the additional rental fee for the set-top, the rental fee only pays for the depreciation on the equipment. FCC regulations limit equipment rental fees to cost.

Wouldn't it be nice if an operator could take his most popular revenue generating movie channel and make it available to all customers on an individual basis using his lowest cost equipment? Positive and negative traps make it possible to do this.

When a particular premium movie channel is so popular that a significant number of lower tier customers would subscribe, it could be profitable for the cable operator to set up the tier arrangement so that the channels can be provided without a set-top converter and without subscribing to an additional tier. Individual channel traps make it possible to do this if the channel is placed in a tier which all subscribers receive.

Case 5. Assume that 3,000 third tier customers currently subscriber to HBO. Also assume that 6,000 out of 10,000 basic subscribers (*Scenario Two*, Table 6.2) would take HBO if it were available. Assume further that 8,000 second tier customers would subscribe if the channel were available to them individually. The *potential* market for the *HBO* channel would be 17,000 subscribers. Using negative traps, the operator would require only 13,000 filters to provide the channel to 17,000 subscribers:

[24] 13,000 x $ 20.00 = $ 260,000.00

The cost of 17,000 set-top converters at $ 75.00 each would be:

SCENARIO FOUR

Table 6.7

Premium Customers:	**5,000**
Total Customers:	**20,000**

[25] 17,000 x $ 75.00 = $ 1,275,000.00

Assume that the premium channel could be sold for around $ 12.00 per month. Yearly revenue for the channel would work out to:

[26] $ 12.00 x 12-months x 17,000 subscribers = $ 2,448,000.00

Consequently, profit for the first year using set-top converters would be $ 1.173-million while profit using single channel traps would be $ 2.188-million. Use of negative traps under these circumstances would increase profits by $ 1.015-million. Clearly, single channel traps have financial advantages in *at least* some circumstances.

In Chapter 3 we saw that a typical drop-line would tolerate the insertion loss of *at least four filters.* Assuming that one of the four filters is a tier filter, an operator would be able to use *at least three more filters* in the drop-line before filter insertion losses become unacceptable. Using one tier filter and individual channel traps, an operator has the capability of providing up to three more individual premium channels to basic customers without using a set-top converter.

Positive vs. Negative Traps

Positive and negative traps provide cable operators with an inexpensive means of supplying individual premium channels *at minimum expense.* Previously we saw how it was possible for a cable operator to place his most popular premium channels in a lower tier so that basic subscribers could receive them individually without using a set-top converter.

Case 6. Suppose the scenario shown in Table 6.6. Using positive traps the operator would require a filter for each premium subscriber. Using negative

NEGATIVE TRAPS PER PREMIUM SUBSCRIBER

Table 6.8

Premium Subscribers	Penetration (Percent)	Non-Premium Subscribers	Traps Per Premium Subscriber
0	0.0	20,000	----
100	0.5	19,900	199
1,000	5.0	19,000	19
2,000	10.0	18,000	9
5,000	25.0	15,000	3
10,000	50.0	10,000	1
15,000	75.0	5,000	1/3
19,000	95.0	1,000	1/19
20,000	100.0	0	0

traps, the operator would require a filter for each non-premium subscriber. Therefore, the operator would require either 11,000 positive traps or 9,000 negative traps:

[27] 9,000 x $ 20.00 = $ 180,000.00

[28] 11,000 x $ 20.00 = $ 220,000.00

[29] / ∴ $ 180,000.00 < $ 220,000.00

Under the circumstances negative filtering could save the operator $ 40,000.00. This corresponds to a savings of 18.18-percent. *In general, when filter prices are equal negative trapping is less expensive than positive trapping whenever penetration exceeds fifty-percent.*

Case 7. Assume the scenario shown in Table 6.7. Under those circumstances, the operator would require either 5,000 positive traps or 15,000 negative filters:

[30] 5,000 x $ 20.00 = $ 100,000.00

[31] 15,000 x $ 20.00 = $ 300,000.00

[32] / ∴ $ 100,000.00 < $ 300,000.00

Under these circumstances positive filters could save the operator $ 200,000. *In general, when filter prices are equal positive trapping is less expensive than negative trapping whenever penetration rates are less than fifty percent.*

POSITIVE vs. NEGATIVE FILTERING*

Table 6.9

Premium Subscribers	Percent Penetration	- Cost ($) - Positive	Negative
0	0	0	400,000
5,000	25	100,000	300,000
10,000	50	200,000	200,000
15,000	75	300,000	100,000
20,000	100	400,000	0

*The table assumes a cable system with 20,000 subscribes and a trap expense of $ 20.00 each.

Using negative filtering, premium subscribers must pay the cost of blocking non-subscribers. When penetration rates are low, negative filtering becomes financially inviable. Table 6.8 illustrates the fact that if one has only one-hundred premium subscribers out of 20,000 subscribers on the system, one would have to purchase 199 negative filters for each premium subscriber.

Cases 6 and 7 make it clear that the most economical method of filtering depends upon penetration rates. In theory, if an operator had one-hundred percent penetration, using negative filtering the operator would not have to purchase any filters at all. Using positive filtering the operator would have to purchase a trap for every subscriber. On the other hand, if an operator had only one premium customer with 19,999 non-subscribers, using positive trapping the operator would only have to buy one filter. Using negative trapping the operator would have to purchase 19,999 filters for non-subscribers. Table 6.9 illustrates the fact that negative filtering is less expensive when penetration rates exceed fifty percent. Positive trapping is less costly whenever penetration rates are less than fifty percent.

So far we have assumed *that positive filters cost the same as negative filters.* Since this may not always be true, cable operators need a general method for finding the point where negative filtering becomes less expensive than positive filtering. The previous estimates neglected to consider installation costs. If installation costs are paid by the subscriber, then we need not include them in our estimates. However, if the costs are paid by the cable operator, then

installation costs can be handled by simply adding them to the cost of filters and set-top converters.

As was done with equations [19] and [20] it is possible to develop *a system of linear equations* for determining the point at which positive and negative filtering costs the same. Hence:

[33] $y = C_n (n - x)$, where:

y = the total cost of negative filtering ($),
x = the number of premium subscribers,
C_n = the cost per negative trap ($),
n = the total number of subscribers in the system.

[34] $y = C_p x$, where:

y = the total cost of positive filtering,
x = the number of premium subscribers, and
C_p = the cost of each positive trap.

By setting equations [33] and [34] equal to each other it is possible to solve for "x" and find the exact point where the two equations intersect:

[35] $y = C_n(n - x) = C_p x$,

Positive and negative trapping each have certain financial advantages depending upon penetration rates and cost. Table 6.10 summarizes their relative advantages and disadvantages. When penetration rates are high, negative trapping methods are usually less costly. However, negative filtering costs are inversely related to revenue. Positive trapping is usually less costly when penetration rates are low. With positive filters, cost are proportional to revenue. For this reason, some operators use positive trapping when they first introduce a new channel and later switch to negative filtering after penetration rates climb. Negative trapping is also useful in small private cable systems with limited resources.

POSITIVE vs. NEGATIVE TRAPPING

Table 6.10

Type	Advantage	Disadvantage
Negative	Lowest cost when penetration rates are high	Higher cost when penetration rates are low
	One of the most secure protections	Costs are inversely proportional to revenue
Positive	Lowest cost when penetration rates are low	Higher cost when penetration rates are high
	Cost proportional to revenue	Less secure than negative filtering

Traps & Tier Filters

There are a variety of *special cases*[2] where negative channel traps may be used in conjunction with tier filters. These cases include:

1. co-location of two premium channels next to each other in the basic tier,

2. locating a negatively trapped channel at the lower *edge* of a second tier, and

3. locating one or more negatively trapped channels in an upper tier.

All of these special cases rely upon making a tier filter do "double duty" in order to significantly reduce the cost of negative channel trapping .

Co-Location. Negative trapping requires putting a filter on each non-subscriber's drop-line. Thus, for a premium channel with a penetration rate of fifty percent in a system with 30,000 subscribers, 15,000 negative traps would be required to block non-subscribers. For two premium channels in the same system with penetration rates of fifty percent, 30,000 negative traps would be needed to block non-subscribers. Using this approach, two negative traps would be required in the drop-lines of subscribers who took neither channel. In the next chapter we will see how it is possible to block two individual

[2]Special case filtering will be explained in greater detail in Chapter 7.

premium channels using a maximum of only one filter in each subscriber's drop-line while still maintaining the capability of supplying all possible channel combinations. The channels selected for this technique should be as low as possible (preferably VHF Channels 2 and 3) because guardband width and trap selectivity declines with increased frequency.

When channels are co-located it is possible to *block both channels using only one wide bandstop filter* (instead of two) on the drop-lines of subscribers who take neither channel. By locating both channels at the bottom of the VHF band, a highpass tier filter can block both channels. Individual channel traps are used on the drop-lines of subscribers who only take one premium channel. No negative traps are required on the drop-lines of subscribers who take both channels. Thus, in some cases this system could halve the cost of negative trapping for high penetration channels depending upon the penetration rates of the four possible channel combinations. Co-location of channels will reduce costs whenever the the following inequality[3] is true:

[36] $$S_t \leq S_1 + S_2 + B,$$ where:

S_t = the total number of systems subscribers,
S_1 = the number of subscribers to the first channel,
S_2 = the number of subscribers to the second channel, and
B = subscribers to both channels.

Edge of Tier Placement. Another way of making tier filters do "double duty" involves locating a premium channel at the bottom edge of the second tier between the first (basic) tier and the second tier. When this is done the tier filter may be used to block the premium channel to non-subscribers. If a basic subscriber takes the premium channel, the first tier filter is replaced with another tier filter which has a higher cut-off frequency. Since the tier filter "doubles" as a negative channel trap, this arrangement uses fewer filters than would otherwise be used to trap a single channel.

THE COST OF CABLE PIRACY

Table 6.11

Tier	Subscribers	Annual Revenue
Basic:	10,000 @ 12 x $ 8.00	$ 0.96-million
Second:	15,000 @ 12 x $ 20.00	$ 3.6-million
Third:	10,000 @ 12 x $ 30.00	$ 3.6-million
Fourth:	5,000 @ 12 x $ 40.00	$ 2.5-million
Totals:	40,000	$ 10.66-million

Upper Tier Placement. Some cable systems have only one premium channel with penetration rates high enough to justify the use of negative traps in the basic tier. When negative trapping is used on the highest filtered tier, penetration rates need only be fifty percent of the upper tier subscribers. Since the filter used to protect the upper tier blocks upper tier premium channels, channel traps need only be used for non-subscribers in the upper tier.

For example, using a lowpass tier arrangement with the penetration rates shown in Scenario One, it would be profitable to negatively trap an upper tier premium channel with only 3,000 premium subscribers. This corresponds to a third tier penetration rate of sixty percent but an *absolute penetration rate of only ten percent.* With 5,000 subscribers on the upper tier, only 2,000 negative traps would be required.

The Cost of Piracy

One way of evaluating filtering costs is to consider the amount of revenue which is lost due to piracy. Estimates of piracy based upon both national surveys and actual system audits typically range between seventeen percent and twenty-five percent of legal subscribers.[4] Consider the subscription rates shown in Table 6.11. The *average* annual revenue per subscriber is $ 271.50. With a piracy rate of twenty percent, the system could easily be losing $ 2.172-

[3]Earl W. Swokowski, ***Fundamentals of Algebra and Trigonometry.*** 4th Edition (Boston, Massachusetts: Pride, Weber, & Schmidt, Inc., 1978), pp. 81-91.

[4]Cf. Chapters 2 and 8 for specific examples.

million per year due to piracy. If tier filtering increased subscription rates by just ten percent, the additional revenue would amount to $ 1.086-million during the first year. If tier filters were used on the taps of 35,000 subscribers and the filters cost $ 10.00 each, the cost of filtering would be $ 355,000. Assuming a system using eight-way taps, installation costs might amount to perhaps $ 5.00 per trap or $ 175,000. It follows that the total cost of installation could run around $ 530,000. Thus, the system could make $ 556,000 in additional revenue while paying for the cost of filtering out of cash flow. Since the filters could be depreciated over a period of time, the investment in filters would eventually be recovered in increased profits.

Developing A Filtering Strategy

We have seen that equipping all subscribers with set-top converters is expensive. We have also seen that tier filtering is usually less expensive than set-top converters unless penetration rates are quite low. In addition, we saw that single channel trapping is less expensive than using set-top converters when customers only take a few premium channels. Positive trapping is usually less expensive when penetration rates are low. Negative trapping is less expensive when penetration rates are high.

Using the methods developed in this chapter it is possible to estimate the exact points at which each option becomes less expensive than its alternatives. Because pay television filters are mass produced, unit prices usually decline with the quantity ordered. All such factors may be calculated in one's strategic filtering model.

Works Consulted

Eagle Comtronics, Inc., "Eagle Traps" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-3.

Eagle Comtronics, Inc., "How To Select A Trap for Premium Channel Control" [Informational Monogram]. Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Campbell R. McConnell, ***Economics.*** 7th Edition. New York: McGraw-Hill Book Company, 1988.

Earl W. Swokowski, ***Fundamentals of Algebra and Trigonometry.*** 4th Edition. Boston, Massachusetts: Pride, Weber, & Schmidt, Inc., 1978.

Chapter 7
System Planning

System planning requires a set of practical guidelines for developing a filtering strategy which will minimize costs and maximize profits. Table 7.1 illustrates a channel guide for a typical 74 channel cable system which uses tier filters, negative channel traps, and positive traps. Some of the channels at the upper end of the spectrum are *duplicated* because the system is in transition from coaxial trunk lines to fiber optical trunk lines. *Some of the set-top converters in the system do not cover the entire cable spectrum.*[1] For financial reasons, the system is phasing these older set-tops out rather than replacing them all with newer units capable of receiving the whole cable spectrum. Thus, subscribers with cable compatible television sets receive duplicate channels.

Much of the tier strategy seen in contemporary cable systems is heavily influenced by the historical requirements of thirty-five channel systems which delivered service to twelve channel television sets. In those systems basic customers were not given set-top converters unless they took second tier channels located in the VHF mid-band (Channels 14 to 22) between Channels 6 and 7. A wide bandstop filter was used as a negative tier filter to block the mid-band. For this reason, some systems use two or three tier filters in their drop-lines and only one single channel trap.

Today, with cable compatible television sets, this arrangement is only necessary to keep basic channels

[1]This illustrates the financial burdens involved with *being heavily invested in costly equipment* which quickly becomes obsolete at a time when major capital investments are required to remain competitive. Replacing all set-tops involves the expense of additional service calls and capital investment without necessarily deriving any additional revenue.

CHANNEL GUIDE
ADELPHIA CABLE COMMUNICATIONS
Syracuse, New York

Table 7.1

2	HBO-1 *	[◦]
3	Public Access	[Basic]
4	WSTM (NBC Syracuse 3)	[Basic]
5	Prevue Guide	[Basic]
6	WIXT (CBS Syracuse 5)	[Basic]
14	Video Classified	[2nd Tier]
15	A & E	[2nd Tier]
16	ESPN	[2nd Tier]
17	USA	[2nd Tier]
18	Nick	[2nd Tier]
19	PPV Information	[2nd Tier]
20	MTV	[2nd Tier]
21	Max-1 * [ASTC]	[2nd Tier]
22	EWTN	[2nd Tier]
7	WNYS (Syracuse 43)	[Basic]
8	WCNY (PBS Syracuse 24)	[Basic]
9	Home Shopping	[Basic]
10	WIXT (ABC Syracuse 9)	[Basic]
11	WSYT (Fox Syracuse 68)	[Basic]
12	WWOR (NYC 9)	[Basic]
13	Local Weather Channel	[Basic]
23	WPIX (NYC 11)	
24	TBS (Atlanta 17)	
25	CNN	
26	Weather Channel	
27	CNBC	
28	CNN-HLN	
29	AMC	
30	Family	
31	Lifetime	
32	TNT	
33	DSC	
34	C-Span	
35	VH-1	
36	BET	
37	TMC * [ASTC]	
38	PPV-1 ** [ASTC]	
39	CNY-2	
40	fX	
41	MS-NBC	
42	E!	
43	EMP	
44	SCNY	
45	MSG	
46	TLC	
47	TCM	
48	FiT	
49	HDTV	
50	History	
51	Food	
52	TNN	
53	ESPN-2	
54	Toon	
55	Comedy	
56	PPV-4** [ASTC]	
57	Sci-Fi	
58	PIN	
59	C-Span-2	
60	Disney* [+]	
61	Show * [ASTC]	
62	Toon	
63	Comedy	
64	PPV-4	
65	Sci-Fi	
66	PIN	
67	C-Span-2 **	
68	TV-Land	
69	International	
70	TV-Land	
71	International	
72	HBO-2 * [ASTC]	
73	HBO-3 * [ASTC]	
74	Max-2 * [ASTC]	

Legend: [Basic] = 1st Tier Basic Service
[2nd Tier] = 2nd Tier Band Stop Filtering
[ ] = 3rd Tier Low Pass Filtering
* = Premium Channel
** = Pay Per View
[◦] = Negative Trapping
[+] = Positive Trapping
[ASTC] = Addressable Set-Top Converter

ordered in logical sequence. Otherwise, it would make more sense to use Channels 2 to 6 and 14 to 19 as a basic tier.

In the last chapter we saw that negative filtering is less costly than set-top converters when penetration rates are high. Positive traps are less expensive than negative traps when penetration rates are low. Since costs are proportional to revenue for both positive traps and set-top converters, positive traps *will always be less expensive than set-tops for a single premium channel.* Set-top converters are cost effective for multiple premium channels when penetration rates are low. Using these principles it is possible to formulate a set of planning guidelines for developing a filtering strategy.

Tier Filtering

Because revenue from commercial satellite channels is low, commercial satellite channels should be combined into groups or tiers. Unless penetration rates are quite low, tier filters are usually less expensive than set-top converters. Since the expense of tier filtering declines with increased penetration, tier channels should be grouped by popularity with the most popular channels in lower tiers and the least popular channels in higher tiers. An example of this technique is shown in Table 7.7. Note that *Time-Warner* has placed some of the *oldest and most popular commercial satellite channels* (like CNN and WTBS) in their second mid-band tier. Since lower penetration channels tend to be more specialized it is more likely that those who really want specialized channels will be willing to pay the additional expense of a set-top converter.

Low Pass Filters. The spectrum between 54 MHz and 1 GHz is divided up into 162 cable television channels. *Theoretically* this spectrum could be subdivided into 162 different tiers using a maximum of *only one lowpass filter per subscriber drop-line.* The minimum number of *different low pass filters* needed for a lowpass tier arrangement is given by the formula:

[1] $n_t = (2^n - 1)$, where:

THREE TIER FILTERING

Table 7.2

Case	-- Tiers* -- 1	2	3	Filtering Requirements
0	0	0	0	None: Disconnect Drop Line
1	1	0	0	LPF
2	1	1	0	LPF
3	1	1	1	None Required

*Legend: 1 = a passband
0 = a stopband
Tiers are represented ascending in frequency.

n_t = the total number of different filters needed, and
n = the number of tiers.

However, with such an arrangement a subscriber taking any particular channel would necessarily *have to purchase all of the channels below the desired channel.* In practice, such a scheme would be impractical because real lowpass filters require a guardband between the passband and the stopband. As the cut-off frequency of a lowpass filter increases, the required guardband widens. Nevertheless, this theoretical scenario illustrates the point that one can create a large number of tiers using a maximum of only one lowpass tier filter per subscriber drop-line. Table 7.2 illustrates a three tier arrangement using this principle.

Other Tier Filters. Highpass filters, bandpass filters, and wide bandstop filters can be used to provide subscribers with any combination of tiers. If one limited the number of channel tiers on a system to three, a cable operator can provide any combination of tiers *using only one filter per drop line.* This fact may be demonstrated logically using the *binary truth table* shown in Table 7.3. Using formula [1], two lowpass filters would be required to separate the tiers. Because no filters are required for the first and last cases, the total number of filters required to provide all possible combinations of tiers is given by the formula:

[2] $n_c = (2^n - 2)$, where:

THREE TIER FILTERING

Table 7.3

Case	-- Tiers* -- 1	2	3	Filtering Requirements
0	0	0	0	None: Disconnect Drop-Line
1	0	0	1	HPF
2	0	1	0	BPF
3	0	1	1	HPF
4	1	0	0	LPF
5	1	0	1	BSF
6	1	1	0	LPF
7	1	1	1	None Required

*Legend: 1 = a passband
0 = a stopband
Tiers are represented ascending in frequency.

n_c = the total number of filters required, and
n = the number of tiers.

Six different filters would be required to provide all possible tier combinations. Since two of these filters would be lowpass filters, four additional high-pass, bandpass, and bandstop filters would be required.

Table 7.4 illustrates the fact that with *four or more tiers*, it is necessary to use the equivalent of *more than one filter* in the drop-line to provide any tier combination. With four tiers, twelve different filters (instead of fourteen) would be required to provide any combination of four tiers. This is because four of the same filters can be reused to provide service for two more tiers.

Thus, filtering four or more tiers is problematic. The equivalent of more than one filter must be used in some drop-lines to deliver all possible tier arrangements. This increases the insertion loss of the drop-line and reduces the number of additional traps which can be used for individual premium channels. Further, the number of different filters needed to deliver all possible tier arrangements starts to become a logistical problem. *It logically follows that to deliver all possible tier combinations with a maximum of one tier filter in the drop-line, the number of filtering tiers must be limited to three.*

FOUR TIER FILTERING*

Table 7.4

Case	--- Tiers* --- 1	2	3	4	Filtering Requirements
0	0	0	0	0	None: Disconnect Drop
1	0	0	0	1	HPF
2	0	0	1	0	BPF
3	0	0	1	1	HPF
4	0	1	0	0	BPS
5	0	1	0	1	HPF & BSF
6	0	1	1	0	BPS
7	0	1	1	1	HPF
8	1	0	0	0	LPF
9	1	0	0	1	BSF
10	1	0	1	0	BSF & LPF
11	1	0	1	1	BSF
12	1	1	0	0	LPF
13	1	1	0	1	BSF
14	1	1	1	0	LPF
15	1	1	1	1	None Required

*Legend: 1 = a passband
0 = a stopband
Tiers are represented ascending in frequency.

Traps & Tier Filters

With certain tier arrangements it is possible to make a single tier filter do "double duty" either by locating *two premium channels* next to each other at the bottom of the VHF band, by *locating a premium channel near the edge of a tier, or* by locating a premium channel *in the highest filtered tier.* This is very desirable because only four filters may be used in a drop-line. Using only one filter to secure two premium channels conserves valuable insertion loss capacity on the drop-line. It also *reduces the cost of securing the channels.* A fifty percent cost reduction could save an operator a *hundred thousand dollars* or more over using individual filters depending upon the system.

Co-Location. If two premium channels are placed on VHF Channels 2 and 3, as illustrated in Table 7.5, a *highpass filter* may be used to block them both. If the subscriber takes only Channel 2,

TRUTH TABLE

Table 7.5

Channel 2	Channel 3	Filtering Requirements
No	No	HPF to block Ch 2 & 3
No	Yes	Trap Ch 2
Yes	No	Trap Ch 3
Yes	Yes	None Required

TRUTH TABLE

Table 7.6

Ch. 14 Premium	Ch. 14 -22 Tier	Filtering Requirements
No	No	Channel 14-22 BSF
Yes	No	Channel 15-22 BSF
No	Yes	Channel 14 Trap
Yes	Yes	None Required

then the highpass is taken off and a single channel notch is placed on Channel 3. On the other hand, if the subscriber takes only Channel 3, then the highpass is taken off and replaced with a notch on Channel 2. Should the subscriber take both channels, then the highpass filter is simply removed. In all cases two channels are blocked using only one negative filter. Use of Channels 2 and 3 for this purpose is desirable because guardband width increases with frequency.

Edge of Tier Placement. In systems which use the mid-band as a second tier, it is possible to make a tier filter do double duty by locating a premium channel near the edge of a mid-band tier. In systems which use a lowpass tier arrangement, the technique may be implemented by locating a premium channel near the lower edge of the *highest filtering tier*.

As noted previously, many cable systems still use the VHF mid-band as a second tier. Actually, this is wasteful because the mid-band stop filter *cannot be used to block all of the tiers above it*. Another low pass tier filter is needed to block all of the channels above Channel 13. Nevertheless the "waste" can be "redeemed," as illustrated in Table 7.6, by locating a premium channel on Channel 14 at the edge of the mid-band. If a subscriber takes neither Channel 14 nor the mid-band tier, then a bandstop filter is used to block Channels 14 to 22. However, if a subscriber takes only the premium channel, then the Channel 14 to 22 bandstop filter is replaced with a Channel 15 to 22 bandstop filter. Alternatively, if the subscriber takes only the mid-band tier without Channel 14, then the Channel 14 to 22 bandstop filter is replaced with a Channel 14 trap.

An actual application of this technique is illustrated in Table 7.7. By locating HBO next to the second mid-band tier, a single negative tier filter can be used for blocking both the second tier and the premium channel. In all cases only one filter is used. A variety of other possible applications of this principle exist depending upon the operator's tier arrangement.

Upper Tier Placement. It is not unusual to find cable systems with only one premium channel (HBO) which has sufficient penetration to justify negative trapping. If a lowpass tier filtering arrangement is used, a maximum of only two negative filters are used in subscriber drop-lines. Under such circumstances, it is sometimes possible to profitably use negative filtering on "low penetration channels" if the channels are placed in the highest filtered tier.

Because the tier filter blocks reception of all tier channels to non-subscribers, lower tier customers do not require individual channel traps for premium channels in a tier to which they don't subscribe. Hence, negative filtering in the highest filtered tier will be profitable when penetration rates are at least fifty percent of the subscribers *on that tier*.

Suppose a system with 30,000 subscribers and 5,000 subscribers on the third tier with two negatively trapped premium channels in the third tier. Negative tier filters block all third tier channels, including the two premium channels, with respect to 25,000 lower tier subscribers. Thus, the premium channels need only have at least 2,500 subscribers to make blocking some 2,500 non-subscribers on the third tier profitable. This corresponds to a third tier penetration rate of fifty percent but an absolute penetration rate of only 8.33-percent.

By placing a negatively trapped upper premium channel at the lower edge of the upper tier, it is possible to make the channels available to customers

CHANNEL GUIDE
TIME-WARNER CABLE
Syracuse, New York

Table 7.7

2	Prevue Guide	[Basic]
3	WSTM (NBC Syracuse 3)	[Basic]
4	Home Shopping	[Basic]
5	WIXT (CBS Syracuse 5)	[Basic]
6	Time Warner High Lights	[Basic]
14	Video Classified	[Basic]
15	HBO-1*	[▫]
16	WTBS (Atlanta 17)	[2nd Tier]
17	WPIX (NYC 11)	[2nd Tier]
18	WGN (Chicago)	[2nd Tier]
19	Animal Planet	[2nd Tier]
20	Family	
21	fX Network	
22	CNN	
7	WNYS (Syracuse 43)	[Basic]
8	WSYT (Fox Syracuse 68)	[Basic]
9	WIXT (ABC Syracuse 9)	[Basic]
10	WCNY (PBS Syracuse 24)	[Basic]
11	WCNY-2	[Basic]
12	Public Access	[Basic]
13	Travel Channel	[Basic]
23	CNN-HLN	
24	ESPN	
25	ESPN-2	
26	TNN	
27	CMTV	
28	MTV	
29	VH-1	
30	Life	
31	USA	
32	DSC	
33	A & E	
34	Nick	
35	C-Span	
36	C-Span 2	
37	CNBC	
38	MS-NBC	
39	E!	
40	Weather Channel	
41	Home Shopping 2	
42	HSN	
43	Odyssey	
44	EWTN	
45	TNT	
46	Food	
47	FiT	
48	BET	
49	TLC	
50	Comedy	
51	Cartoon	
52	Court TV	
53	Si Fi	
54	Sports	
55	AMC	[ASTC]
56	MSG	[ASTC]
57	Golf	[ASTC]
58	PPV-Previews	[ASTC]
59	fXM	[ASTC]
60	H & G	[ASTC]
61	Program Guide	[ASTC]
62	History	[ASTC]
63	TMC	[ASTC]
64	Encore	[ASTC]
65		
66	HBO-2*	[ASTC]
67	HBO-3*	[ASTC]
68	Cinemax*	[ASTC]
69	Cinemax-2*	[ASTC]
70	TMC*	[ASTC]
71	Disney*	[ASTC]
72	Showtime*	[ASTC]
73	Viewer's Choice **	[ASTC]
74	Continuous Choice**	[ASTC]
75	Hot Choice**	[ASTC]
76	Spice**	[ASTC]

Legend: [Basic] = 1st Tier Basic Service
[2nd Tier] = 2nd Tier Band Stop Filtering
[ ] = 3rd Tier Low Pass Filtering
* = Premium Channel
** = Pay Per View
[▫] = Negative Trapping
[+] = Positive Trapping
[ASTC] = Addressable Set-Top Converter

on the lower tier by simply using a tier filter with a higher cut off frequency.

Channel Traps

Single channel traps make it possible to economically deliver both high and low penetration premium channels to subscribers on an individual basis without using a set-top converter box.

Negative Traps. Previously we saw that negative trapping is economical for high penetration premium channels. Although simplified theoretical models illustrated the fact that negative trapping is economical when penetration exceeds fifty percent, *some trap manufactures recommend penetration rates of at least fifty-five percent.* The additional five percent provides some margin for disconnects during recessions and takes installation costs into consideration.

In order to maximize penetration, *high penetration premium channels should be placed in the basic tier which all subscribers receive so that they can be provided to any subscriber without a set-top converter.* Both of the systems illustrated in Tables 7.1 and 7.7 use this principle for delivering HBO.

Positive Traps. We have seen that positive trapping of *a single channel* will always be less expensive than using a set-top converter. When VHF positive trapping is used, placement on the lowest possible channel will minimize picture degradation. Low tier placement will also make the channel accessible to all viewers.

Since the revenue derived from a positively trapped channel depends upon the number of subscribers taking the channel, the number of subscribers taking the channel will probably be higher if the channel is easily accessible on an individual basis to all subscribers on the system. *It logically follows that, where feasible, positively trapped*

channels should be placed on the lowest channel possible in the lowest tier to avoid complications in making the channel accessible to all customers.

If positive trapping is used in the super-band, with a system like Arcom's *Gaussian system, SAWDEC,* or Eagle's *Sideband Interdiction System*, positive traps may be used on higher channels. However, the channel may not be accessible to all subscribers. Thus, some subscribers may have to take an additional tier.

Although it is highly desirable to place positively trapped channels in lower tiers, there are situations in which lower tier placement may not be justified by revenue and penetration rates. For example, if an operator is using a highpass tier filter and three negative traps in the basic tier, it may not be possible to add the insertion loss of *an additional filter* to subscriber drop-lines without creating reception problems for some subscribers.

In the Adelphia system illustrated in Table 7.1, positive super-band filtering is used for *Disney* on channel 60. Because the subscription fee for the channel is relatively low when compared with other premium channels, the revenue generated by the channel is relatively low when compared to other premium channels with comparable penetration rates. Where Adelphia charges $ 12.00 per month for HBO and $ 11.50 per month for all other premium channels, the charge for the Disney Channel is only $ 8.95 per month. An additional set-top converter rental fee for such a low cost channel would probably kill many sales for a channel which already has low penetration. Thus, higher tier placement is justified.

There is one engineering advantage to placing a positively trapped channel in an upper tier when certain tier filtering schemes are used. If one assumes a system using one tier filter and three single channel traps, an additional positive trap in basic tier drop-lines could exceed the insertion loss capacity of the lines. However, because the tier filter is removed on the highest tier, there is *room for an additional filter* without exceeding the insertion loss capacity of the drop-line. Depending upon the tier arrangement, the only limitation is that subscribers might have to take all tiers before they receive a positively trapped channel on an upper tier. Thus, *positive super-band trapping systems have certain advantages with lower cost low penetration premium channels.*

Set-Top Converters & Addressable Taps

Because set-top converters and addressable taps are relatively costly they should be reserved for applications which either cannot be performed economically using filters or which cannot be performed at all using filters. Such applications include -

1. providing *PPV or IPPV services*,
2. securing any *low penetration tiers* which cannot be secured economically with tier filters
3. deciphering low *penetration premium channels*,
4. securing *premium channels* which cannot be secured using filters, and
5. delivering *multiple premium channels* which cannot be secured economically with traps.

Because basic subscribers do not require set-tops and because set-tops are capable of deciphering high frequency channels; *premium channels, PPV channels, and IPPV channels secured with set-tops should be placed in upper tiers* as illustrated in Table 7.7.

If *commercial satellite channels* are ordered along the spectrum by penetration rate, then low penetration channels will fall in the higher tiers and high penetration channels will fall in lower tiers. The systems shown in Table 7.1 and 7.7 both place most of their low penetration premium channels and all of their PPV channels in upper tiers.

By using this approach, the commercial satellite channels are protected by the last tier filter. Premium channels, PPV channels, and IPPV channels are secured with respect to third tier customers by encryption at the headend. Third tier premium channels, PPV channels, and IPPV channels are secured with respect to lower tier subscribers by *both the tier filters and encryption at the headend.* Hence, a cable pirate must at least purchase the highest tier before receiving the enciphered signals of the

premium channels.

As previously noted, it is possible to subdivide the third tier making a fourth tier using the set-top converter. Fourth tier commercial channels may be enciphered at the headend and deciphered with the set-top converter. Note that the *Time-Warner* system illustrated in Table 7.7 also uses the set-top converter to establish a *fourth low penetration tier* above Channel 54.

General Guidelines

The foregoing considerations allow us to develop a set of step-by-step guidelines for using filters to secure television channels at minimum expense. These guidelines are listed in Table 7.8. Although it may not always be possible to adhere to the letter of these guidelines, following most of them will lower costs and increase profits.

Table 7.9 illustrates a hypothetical cable system designed using the guidelines listed in Table 7.8. The design *presumes that four premium channels have penetration rates over fifty-five* percent. Although this is seldom the case with contemporary cable systems, the hypothetical case *illustrates the capability of filters to secure a considerable number of high penetration premium channels* before using set-top converters or addressable taps.

Three tiers are secured with lowpass filters. The fourth tier is secured using headend encryption and set-top converters. The system is designed to use a maximum of four filters in drop-lines. Positive filtering of *Disney* in the third tier is made possible by

SYSTEM DESIGN GUIDELINES

Table 7.8

1. Make three tiers using lowpass filters. Cut-off frequencies should be assigned after channel allocation to the three tiers.

2. Determine the expected penetration of all premium channels. If necessary, consult a neighboring system to determine their penetration rates for the same channels or do a marketing survey.

   a. If there is only one premium channel with a penetration rate of fifty-five percent or more, allocate the channel to Channel 2 on the first tier. Allocate all other channels to the third tier.

   b. If three or more channels have penetration rates of fifty-five percent or more, order them by penetration and assign the top three to the first tier.

   c. If more than four premium channels have equal penetration rates greater than fifty-five percent, consider placing the oldest four channels in the basic tier using the technique illustrated in Table 7.5 or Table 7.6. Otherwise, place the oldest three in the basic tier for negative trapping and allocate the rest to the third tier.

3. Allocate all local broadcast channels to the basic tier and complete basic tier allocations.

4. Order all commercial satellite channels by penetration rate.

   a. Allocate commercial satellite channels with penetration rates greater than fifty-five percent to the second tier.

   b. Allocate all commercial satellite channels with penetration rates of less than fifty-five percent to the third tier.

5. If drop-line insertion loss capacity permits, place any premium channels allocated to the third tier with expected penetration rates greater than fifty-five percent on the lower edge of the second tier.

6. Calculate the expected third tier penetration rates of all premium channels allocated to the third tier. If drop-line insertion loss capacity permits use negative trapping on any third tier premium channels with third tier penetration rates in excess of fifty-five percent. Place these channels on the lowest third tier channels possible.

7. If drop-line insertion loss capacity permits, assign the most popular low penetration premium channel to the third tier for positive trapping.

8. Order third tier commercial satellite channels by penetration rate with the highest penetration channels at the bottom of the third tier and the low penetration channels at the top of the tier.

9. Create a fourth tier using headend encryption and set-top converters.

   a. Assign all low penetration rate commercial satellite channels to the fourth tier.

   b. Assign all unfiltered premium channels to the fourth tier.

   c. Assign all PPV and IPPV channels to the fourth tier.

CHANNEL GUIDE
HYPOTHETICAL CABLE SYSTEM # 1
Syracuse, New York

Table 7.9

2	HBO*	[-]	25	WTBS (Atlanta 17)	[2nd Tier]	51	Cartoon	
3	Cinemax	[-]	26	TNT	[2nd Tier]	52	USA	
			27	ESPN-1	[2nd Tier]	53	TNN	
4	WNYS (Syracuse 43)	[Basic]	28	ESPN-2	[2nd Tier]	54	CMTV	
5	WTVH (CBS Syracuse)	[Basic]	29	Weather Channel	[2nd Tier]	55	E!	
6	Showtime*	[-]	30	C-Span-1	[2nd Tier]	56	EWTN	
			31	C-Span-2	[2nd Tier]	57	Animal Planet	
14	TMC*	[-]	32	WGN (Chicago)	[2nd Tier]	58	fX	
15	Prevue Guide	[Basic]	33	MTV	[2nd Tier]	59	Sports Channel	[ASTC]
16	Video Classified	[Basic]	34	VH-1	[2nd Tier]	60	Odyssey	[ASTC]
17	Local Weather	[Basic]	35	Program Guide		61	H & G	[ASTC]
18	Travel Channel	[Basic]	36	Disney*	[+]	62	Comedy	[ASTC]
19	Public Access	[Basic]				63	Food	[ASTC]
20	WCNY (PBS Syracuse 24)	[Basic]	37	CNBC		64	Golf	[ASTC]
21	WCNY-2	[Basic]	38	MSNBC		65	Court TV	[ASTC]
22	WWOR (NYC 9)	[Basic]	39	A & E		66	MSG	[ASTC]
			40	TLC		67	fXM	[ASTC]
7	HSN	[Basic]	41	DSC		68	Encore	[ASTC]
8	WSYT (Syracuse 68)	[Basic]	42	TCM		69	PPV Previews	[ASTC]
9	WIXT (ABC Syracuse 9)	[Basic]	43	History		70	HBO-2*	[ASTC]
10	Shopping - 1	[Basic]	44	Nick		71	HBO-3*	[ASTC]
11	WPIX (NYC 11)	[Basic]	45	BET		72	Cinemax-2*	[ASTC]
12	Shopping - 2	[Basic]	46	Lifetime		73	Viewer's Choice**	[ASTC]
13	WSTM (NBC Syracuse 3)	[Basic]	47	Family		74	Continuous Hits**	[ASTC]
			48	AMC		75	Hot Choice**	[ASTC]
23	CNN	[2nd Tier]	49	FiT		76	Spice**	[ASTC]
24	CNN-HLN	[2nd Tier]	50	Sci Fi				

Legend: [Basic] = 1st Tier Basic Service
[2nd Tier] = 2nd Tier Band Stop Filtering
[ ] = 3rd Tier Low Pass Filtering

* = Premium Channel
** = Pay Per View

[-] = Negative Trapping
[+] = Positive Trapping
[ASTC] = Addressable Set-Top Converter

the fact that the third tier lowpass filter is removed for customers taking the third. One disadvantage of this design is that customers taking Disney must take at least the third tier.

The system illustrated in table 7.10 was designed using the principle in Table 7.8 under the assumption that *only one premium channel has sufficient penetration to justify negative trapping on the basic tier.*

Works Consulted

Adelphia Cable Communications, "Cable Programming Rates & Services [Program Guide Card]." Syracuse, New York: Adelphia Cable Communications, 1996.

George Boole, ***An Investigation of the Law Of Thought On Which Are Founded The Mathematical Theories of Logic And Probabilities [1854].*** New York: Dover Publications, 1958.

Irving M. Copi, ***Introduction to Logic.*** 5th Edition. Belmont, California: MacMillan Publishing Company, Inc., 1978.

Eagle Comtronics, Inc., "How To Select a Trap for Premium Channel Control [Informational Monogram]." Clay, New York: Eagle Comtronics, Inc., nd., pp. 1-2.

Thomas L. Floyd, "Boolean Algebra" in ***Digital Fundamentals.*** 4th Edition. Columbus, Ohio: Merrill Publishing Company, 1990, pp. 144-80.

Howard Kahane, ***Logic And Philosophy.*** 3rd Edition. Belmont, California: Wadsworth Publishing Company, Inc., 1978.

Time-Warner Cable, "Channel Lineup [Program Guide Card]." East Syracuse, New York: Time-Warner Communications, 1996.

CHANNEL GUIDE

HYPOTHETICAL CABLE SYSTEM # 2

Syracuse, New York

Table 7.10

2	HBO*	[-]	25	WTBS (Atlanta 17)	[2nd Tier]	51	Cartoon	
3	WSTM (NBC Syracuse 3)	[Basic]	26	TNT	[2nd Tier]	52	USA	
			27	ESPN-1	[2nd Tier]	53	TNN	
4	WNYS (Syracuse 43)	[Basic]	28	ESPN-2	[2nd Tier]	54	CMTV	
5	WTVH (CBS Syracuse)	[Basic]	29	Weather Channel	[2nd Tier]	55	E!	
6	Prevue Guide	[Basic]	30	C-Span-1	[2nd Tier]	56	EWTN	
			31	C-Span-2	[2nd Tier]	57	fX	
14	Local Weather		32	MTV	[2nd Tier]	58	Odyssey	[ASTC]
15	Video Classified	[Basic]	33	VH-1	[2nd Tier]	59	H & G	[ASTC]
16	WGN (Chicago)	[Basic]	34	Cinemax*	[-]	60	Comedy	[ASTC]
17	Shopping - 1	[Basic]	35	Showtime*	[-]	61	Food	[ASTC]
18	Shopping - 1	[Basic]				62	Golf	[ASTC]
19	HSN	[Basic]	36	Program Guide		63	Court TV	[ASTC]
20	WCNY (PBS Syracuse 24)	[Basic]	37	CNBC		64	MSG	[ASTC]
21	WCNY-2	[Basic]	38	MSNBC		65	fMX	[ASTC]
22	WWOR (NYC 9)	[Basic]	39	A & E		66	Encore	[ASTC]
			40	TLC		67	PPV Previews	[ASTC]
7	Travel Channel	[Basic]	41	DSC		68	Disney*	[ASTC]
8	WSYT (Syracuse 68)	[Basic]	42	TCM		69	TMC*	[ASTC]
9	WIXT (ABC Syracuse 9)	[Basic]	43	History		70	HBO-2*	[ASTC]
10	Public Access	[Basic]	44	Nick		71	HBO-3*	[ASTC]
11	WPIX (NYC 11)	[Basic]	45	BET		72	Cinemax-2*	[ASTC]
12	Lifetime	[Basic]	46	Sports Channel		73	Viewer's Choice**	[ASTC]
13	Animal Planet	[Basic]	47	Family		74	Continuous Hits**	[ASTC]
			48	AMC		75	Hot Choice**	[ASTC]
23	CNN	[2nd Tier]	49	FiT		76	Spice**	[ASTC]
24	CNN-HLN	[2nd Tier]	50	Sci Fi				

Legend: [Basic] = 1st Tier Basic Service
[2nd Tier] = 2nd Tier Band Stop Filtering
[ ] = 3rd Tier Low Pass Filtering

* = Premium Channel
** = Pay Per View

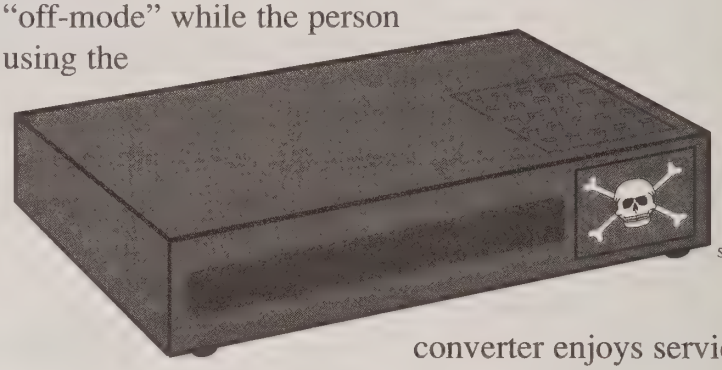
[-] = Negative Trapping
[+] = Positive Trapping
[ASTC] = Addressable Set-Top Converter

Chapter 8
Cable Piracy

In 1992 the *National Cable Television Association* (NCTA) estimated that 9.4-million illegal users received "basic" cable services in the United States.[1] The NCTA further estimated that 6.4-million illegal users received premium services. These estimates were based upon a national survey of 2,684 cable systems conducted during June 1992. Although cable piracy has always been a problem, the growth of cable television since 1982 has accelerated piracy to epidemic proportions. The illegal sale of set-top converters has become big business involving millions of dollars annually.

The extent of the piracy problem is illustrated by a *Time-Warner* audit in New York City. An audit of some 246,541 locations identified some 53,771 illegal subscribers connected to the system using 9,141 pirate set-top converters.[2] In terms of taps, that amounts to a piracy rate of 21.8-percent. With some 192,777 legal subscribers on the system, pirates were around 17.9-percent of the viewers connected to the system. That is equivalent to *a pirate to subscriber ratio* of 1:3.6. Almost 17-percent of the illegal viewers were using pirate set-top converters.

The use of pirate converters has become a serious and widespread problem. For example, near Oxnard, California, a local electronics school was distributing schematics of the set-tops used by *Jones Intercable* to its students. The students, in turn, were using them to modify converters for premium reception.[3] However, the problem of piracy has gone well beyond a few students modifying converters. Pirate manufacturers have gone so far as to make special computer chips which can be substituted in authorized set-tops to decipher any premium channel.[4] Systems with addressable converters have found their converters modified so that the cable system computer continually reads them as being in the premium "off-mode" while the person using the



converter enjoys service from all premium channels.[5]

In three prosecutions of pirate distributors operating in Florida, New York, and Arizona some 35,000 pirate "decoders" were reportedly confiscated.[6] In October 1990, federal marshals reportedly seized 50,000 illegal "decoders" in New York City.[7] In June 1992, the *Los Angeles Police Department* (LAPD) seized 10,000 pirate "decoders" in searches using five warrants.[8] During August 1992 the *Federal Bureau of Investigation* (FBI) seized another 40,000 pirate "decoders" in San Francisco.[9] In October 1992, authorities confiscated 70,000 pirate "decoders" during raids in Los Angeles and Las Vegas.[10] In another case involving an alleged pirate distributor in Ohio, the FBI documented some $ 4,270,233 in sales over a three year period.[11]

If the *Time-Warner* case in New York City represents the level of piracy among households illegally connected to a system, one might wonder *how many pirate set-tops are in the hands of paying subscribers?* No one really knows but the rate is believed to be high. *It is very difficult to determine*

[1]National Cable Television Association, ***Signal -Security Handbook: A Resource Manual for Cable-Operators.*** p. 1.

[2]Kathleen Scoop, Barry Rosenblum, and Daniel J. Lefkowitz, "Time-Warner Cable NYC Attacks Theft At All Levels" in ***CED***. June 1996. pp. 100, 102.

[3]Bill Rivas, "Jones Intercable's Theft of Cable Amnesty Program" in ***CED***. June 1996. p. 94.

[4]Paul Paradise, "Signal-Theft" in ***Electronic Now***. January 1995. p. 39.

[5]NCTA, p. 38.

[6]Scoop, et. al., pp. 100, 102.

[7]NCTA, p. 59.

[8]Mike Bates and Robert Depweg, "How Continental of LA Thwarted Complex Piracy Ring" in ***CED***. June 1994. p. 60.

whether an authorized subscriber is using a pirate set-top converter to receive unauthorized premium channels.

Occasionally, when a pirate distributor is arrested it is possible to determine from confiscated business records who purchased pirate set-tops. However, because some set-tops are so easily modified, unauthorized modification of *authorized converters* is common. Frequently, small time operators exchange unmodified set-tops for modified set-tops as part of the sale in order to maintain a continuing stock of converters. There is also a big *black market* in stolen set-tops. Drug addicts who burglarize homes and apartments pick-up the converters along with the television sets and stereos. The televisions and stereos are sold to the "hock-shop" and the converters are sold to the local piracy ring.

The cable operator's first clue that something funny is going on may occur when a customer disconnects and returns a converter with a different serial number from the one issued. When technicians examine the converter they discover that it has been modified to receive all premium programming. Or, a customer may simply report a modified converter as "stolen" while downgrading to "basic services." Table 8.1 lists a number of symptoms of piracy.

Some view cable television's initial foray into the field of *communications security* (COMSEC) as a complete fiasco. Manufacturers and cable operators are learning the hard way what generations of cryptographers have repeatedly relearned during the last two thousand years. *"Never under estimate the knowledge, skill, or technological sophistication of an opponent."* The worst aspect of the whole situation is that all of these developments could have been foreseen by anyone with professional training in the field of communications security.

In response to cable piracy, many cable systems have implemented elaborate "amnesty campaigns" intended to convert pirates into paying subscribers.[12] One might wonder why the operators just don't replace their set-tops with converters which use more sophisticated cipher systems? The answer is that replacement is just too expensive. Replacing just 10,000 converters at $ 75.00 each could cost a cable system $ 750,000 for set-tops and another $ 400,000 for installation before considering the cost of headend equipment, computer programming, and a variety of other expenses. Further, since *no cipher system is "unbreakable" and because program security systems are inherently vulnerable to analysis*, the operator has no assurance that a new system will not be compromised six months to a year after it is installed. Thus, *an over dependence upon set-tops for security is both risky and expensive.*

SYMPTOMS OF PIRACY*

Table 8.1

1. **Reports of traps missing from drop-line traps.**
2. **Reports of illegal devices connected to taps.**
3. **An usual number of customers reporting lost or stolen converters.**
4. **High converter or positive-trap losses in the warehouses.**
5. **Returned converters which show signs of modification or tampering.**
6. **Returned converters with serial numbers which do not match those issued.**
7. **A significant increase in the number of disconnects.**
8. **Significantly lower penetration rates for premium channels than those of adjacent systems.**
9. **Requests for PPV guides from customers which are not signed up for PPV services.**

***After Bill Rivas, "Jones Intercable's Theft of Cable Amnesty Campaign" in *CED* June 1986. p. 96.**

Some operators have successfully implemented programs for identifying pirate set-top users. Such programs involve transmitting a program which only unauthorized set-top converters can receive. Commands are sent to authorized set-tops to automatically switch to a different channel to receive the same program. A special offer is placed on the channel which only unauthorized viewers receive. By

[9]NCTA, p. 58.

[10]Bates & Depweg, p. 60.

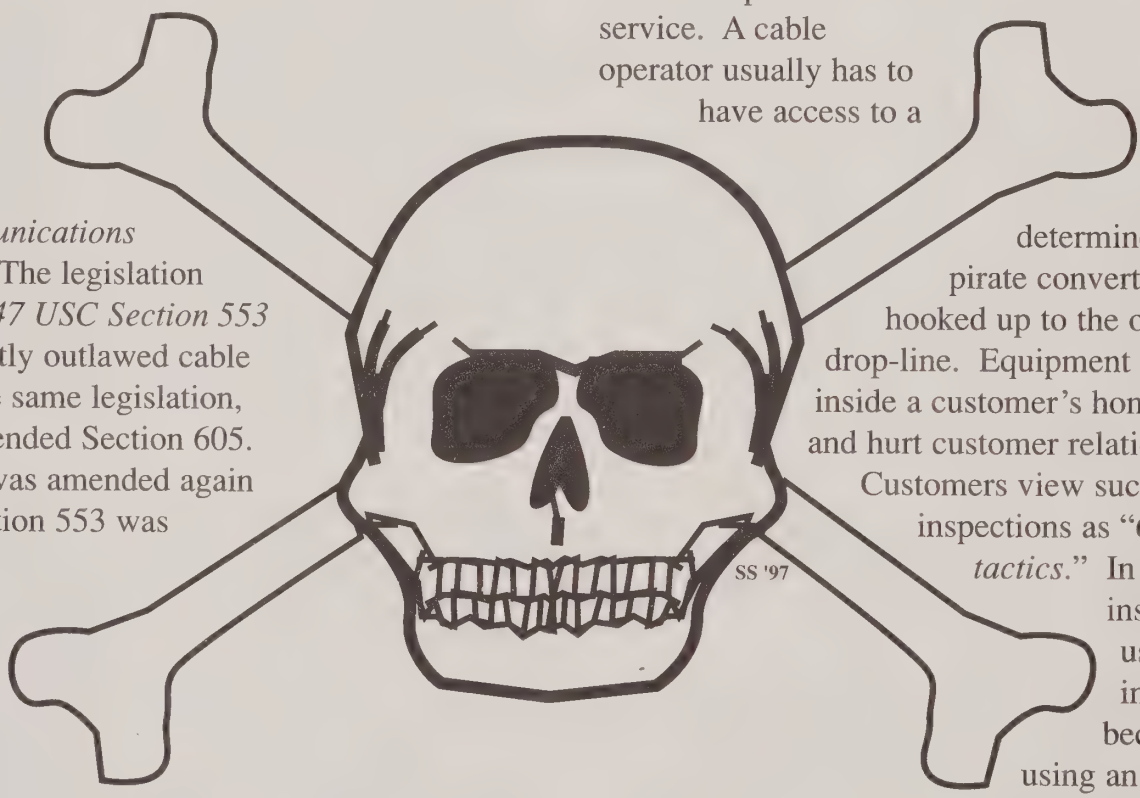
[11]Bates & Depweg, p. 59.

[12]The NCTA publishes an educational kit for cable operators in cooperation with the Coalition to Oppose Signal-Theft. The kit is designed to implement a complete anti-piracy campaign with pre-written news releases, radio spots, advertisements, leaflets, letters, and even door-knob hangers. Cf. National Cable Television Association and the Coalition to Oppose Signal Piracy, ***Cable-Theft is a Crime: Educational Kit.***

calling a special number, the viewer can receive a free gift. When pirate viewers call to receive their free gift, the cable system is able to identify their addresses.

Piracy Law

Most of the piracy prosecutions since 1984 have relied upon relatively new legislation. Prior to 1984, the only federal law prohibiting cable piracy was contained in *Title 47 United States Code (USC) Section 605*. Because that statute was originally written to protect private radio communications as part of the *Communications Act of 1934*, some prosecutors were uncertain as to whether the section was applicable to piracy on a closed circuit cable system.



In 1984, Congress clarified the law in the *Cable Communications Act of 1984*. The legislation created *Title 47 USC Section 553* which explicitly outlawed cable piracy. In the same legislation, Congress amended Section 605. Section 605 was amended again in 1988. Section 553 was amended as part of the *Cable TV Consumer-Protection Act of 1992*. In addition to federal prosecution, federal law also gives injured cable operators *legal standing* to take private *civil action* in either the state or federal courts.

Whenever a pirate distributor uses *a means of interstate commerce* - like the U.S. Mail or interstate telephone lines - prosecution is sometimes possible under federal mail and wire fraud statutes.[13] Large distributors can also be prosecuted under the *Racketeering, Influence, and Corrupt Organizations* (RICO) *Act*.[14] In addition to these federal statutes, most states have enacted anti-piracy laws.[15]

Types of Piracy

Cable television piracy has been divided into a variety of different categories and subcategories by various analysts for analytical purposes. For the purpose of system design, pirates may be divided into two groups - (1) unauthorized viewers, and (2) authorized subscribers.

Because some unauthorized viewers hook up their own drop-lines, they are easily detected through periodic tap audits. Piracy among authorized subscribers is sometimes more difficult to detect because they have authorized drop-lines and pay for some level of service. For example, a subscriber may pay for basic-service and then use a pirate-converter to receive premium service. A cable operator usually has to have access to a residence in order to determine whether a pirate converter box is hooked up to the other end of the drop-line. Equipment inspections inside a customer's home are costly and hurt customer relations. Customers view such inspections as "*Gestapo tactics*." In any event, inspections are usually ineffective because a pirate using an illegal set-top can just disconnect the illegal converter before the inspection and reconnect it after the inspection. Certain drop-line tests have been developed to detect certain pirate converters but such tests are often inconclusive and depend upon the nature of the pirate equipment being used.

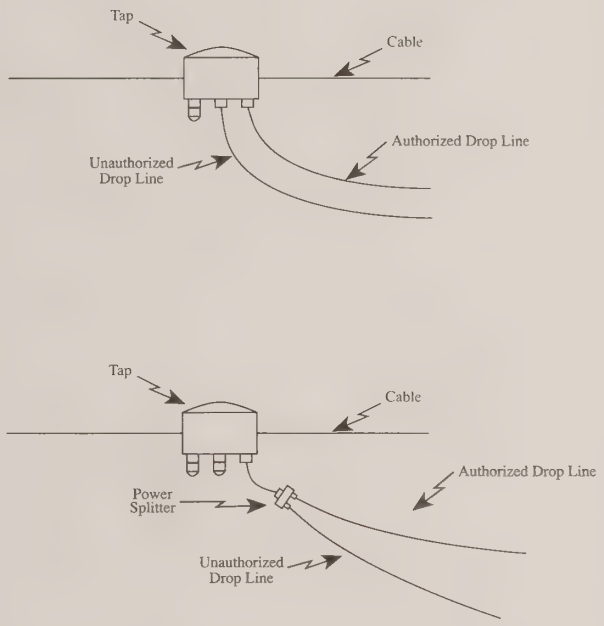
[13]***Title 18 USC Sections 1341 to 1346.***

[14]***Title 18 USC Sections 1961 to 1968.***

[15]The National Cable Television Association's ***Signal - Security Handbook*** contains a data-retrieval chart of State piracy laws in addition to the texts of ***Title 47 USC Sections 553 and 605.***

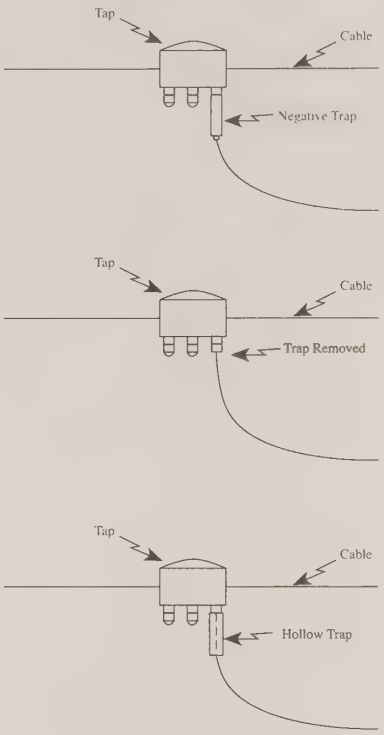
METHODS OF DROP-LINE PIRACY

Figure 8.1



METHODS OF DROP-LINE PIRACY

Figure 8.2



Unauthorized Viewers. Most forms of piracy among unauthorized viewers are detectable because they have to hook-up an illegal drop-line. Such pirates typically hook-up their own drop-lines using one of several techniques. When taps are not locked, a pirate can just climb a telephone-pole and hook-up his own drop-line. To try to preclude this from happening, many cable operators use locking terminators on their unused taps. In that case, the pirate simply cuts the nearest *authorized drop-line* and inserts a power-divider purchased from any electronics supply store. When no taps are available, some pirates have been known to drive a nail through a quarter-inch feeder-line to connect up their drop. Needless to say, such holes leak signals.

Although no form of piracy is desirable, this kind of piracy is preferable to the use of a pirate converter *because it is detectable*. It can also be easily documented to prosecute the offender. Routine tap audits can uncover illegal drop-lines or unauthorized splitters. Unauthorized cable penetrations can be detected with a cable-leakage detector. Because a leak in the shield of a coaxial cable will cause both "*egress*" and "*ingress,*" leaks will sometimes start causing reception problems for subscribers in the area.

Drop-line piracy is sometimes carried out by illegal hook-up installers who offer to hook-up unauthorized viewers for a fee. There have also been schemes where authorized cable installers hook-up customers for a fee without reporting the installation to the cable system. In some cases illegal hook-up installers use equipment stolen from the cable company so that their equipment looks the same as the equipment used by the local cable operator.

Occasionally, in large urban apartment complexes, it is necessary to run drop-lines or feeder-lines through buildings in order to reach subscribers' apartments. In such circumstances, it may be more difficult to detect unauthorized drops-lines without the cooperation of the building management.

Authorized Subscribers. Unlike piracy among unauthorized subscribers, authorized subscribers are paying for some level of cable service. Piracy among authorized subscribers may be subdivided into two categories - (1) *detectable* piracy, and (2) *undetectable* piracy. For example, an authorized subscriber who removes a pay television filter from a tap is detectable. However, an authorized subscriber who uses a pirate set-top converter may be practically undetectable. *Use of unauthorized positive traps is*

equally difficult to detect.

Most cable operators use locking devices to lock their filters to the subscriber's tap so they cannot be easily removed. However, pirates have been known to break filters off a tap or remove them using a hack-saw. Because this kind of subscriber piracy is detectable during a tap audit, some pirates have been known to use even more clever techniques. Instead of just removing the filter, some pirates have been known to "drill" the cylinder using a power drill. The drop-line is then run through the hollow filter enclosure and connected to the tap. From the ground, it looks like there is a filter on the customer's tap. Hence, close inspection of taps is sometimes necessary to detect piracy.

The Positive Piracy System

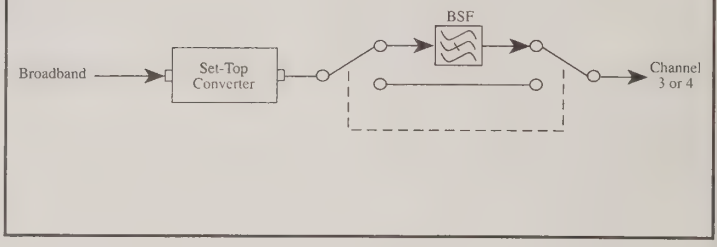
It has been observed that a positive security system is easily defeated if a pirate can steal, purchase, or fabricate an appropriate trap. *A pirate trap distributor does not have to carry 71 different positive-traps in order to sell illegal service for any positively trapped channel.* Figure 8.3 illustrates one of the reasons that the TEST security system is so vulnerable to compromise.

By obtaining a positive trap for either Channel 3 or Channel 4, a pirate can mount the trap on the output of a generic set-top converter with a set of A/B switches to receive any positively trapped channel. Generic converters are commonly available at stores like the *Radio Shack* for use on older television sets. Because all channels are down-converted to the modulator output channel, the jamming carrier on all channels will be down-converted to the same notch frequency on either Channel 3 or 4. The A/B switch is used to by-pass the positive filter when the converter is used on regular channels. Hence, *a pirate can obtain any positively trapped channel with just one filter.*

This is one of the reasons why filter manufacturers restrict the sale of their positive-traps to only *bonafide* customers. However, because the notches used with the TEST security system are so easily duplicated, it is not very difficult for a technician to build one. The de-emphasis filters used with *Arcom's Gaussian* system and *Eagle's Sideband*

THE POSITIVE PIRACY SYSTEM

Figure 8.3



Interdiction System are more difficult to duplicate.

Because positive security systems are so vulnerable to piracy, *it is a bad idea to mount positive filters inside set-top converters.* If the converter is "lost" or "stolen" and the cable operator loses control of the trap, anyone who has the trap can recover the channel anywhere on the system for as long as the system is used. It is also conceivable that the trap could be analyzed and duplicated in large quantities. *Positive traps should always be locked to taps or locked inside pedestal boxes.* Positive trap inventory within the cable system should also be closely controlled to prevent employee theft. When a positive security system is used on an upper tier protected with tier filters, the security of the tier filter will add to the security of the positive-system *on lower tiers.*

Electronic Countermeasures. It was observed in Chapter 3 that addressable set-top converters which rely upon periodic authorization codes or program tags can be easily defeated by disabling certain circuits inside the converters. Two-way systems which detect unauthorized set-tops by asking each set-top its serial number can be defeated in a similar way.

Jerrold Communications has successfully figured out how to use a *computer "virus"* or an "*electronic bullet*" to destroy the circuity in some unauthorized set-tops connected to a cable system.[16] Basically, this is done by having the headend computer send out two commands. The first command tells all authorized set-tops to ignore the

[16]Cf. NCTA, p. 41, and Paradise, p. 39.

SCENARIO ONE

Table 8.2

Tier	Subscribers	Security
Basic	20,000	Drop-Line
Second	15,000	ASTC
Third	10,000	ASTC
Fourth	5,000	ASTC
Total:	50,000	

SCENARIO TWO

Table 8.3

Tier	Subscribers	Security
Basic	20,000	Drop-Line
Second	15,000	Tier Filters
Third	10,000	Tier Filters
Fourth	5,000	ASTC
Total:	50,000	

next command addressing each authorized set-top by its serial number. The second command tells the microprocessor inside the set-tops to "destroy themselves." Since all authorized set-tops have received an addressable command to ignore the second command, only the unauthorized set-tops implement the second command. The success of this method is closely linked to the design of pirate "decoders." It will only work when a very specific pirate microprocessor chip is installed. However, the success of the method points the way for options in future set-top designs.

If a "self-destruct" feature were subtly built into the design of all set-top micro-processors, it would make it possible to destroy stolen set-tops when they are connected to a system. Although the circuits inside the set-top could still be disabled to prevent the set-top from implementing the commands, the feature could increase the amount of information and sophistication a pirate has to have to do illegal conversions successfully.

Using Filters To Limit Piracy

Although pay television filters cannot stop pirates from connecting up illegal drop-lines or driving nails through feeder lines, they can *help* stop piracy in three ways. First, filters can be deployed to make piracy more *detectable*. Second, filters can be used to enhance the security provided by set-top converters and positive security systems. Third, filters can be used to *limit* the amount of piracy occurring within a system.

Detection. Consider the system represented in *Scenario One*, *Table 8.2*. *The system* uses 30,000 converters to decipher all channels except the basic tier. Any customer who has a pirate set-top can receive all channels. If a pirate signs up for basic service and uses a pirate set-top converter, the compromise is virtually undetectable. The whole system is "wide open" to piracy. Because the set-tops inflate the cost of service, subscription rates are higher, fewer people subscribe, and the incentive for piracy is high.

Now consider the system illustrated in *Scenario Two*, Table 8.3. The system uses 35,000 lowpass tier-filters and only 5,000 converters. Rates can be lower and the incentive for piracy is low. Also, because fewer set-tops are used, more sophisticated set-tops can be purchased. If lowpass tier traps are used, a pirate authorized to receive premium service may remove the tier filter and connect up a pirate converter, but in doing so the *pirate has left tell-tale evidence* which can be detected and documented during a routine audit.

Both systems have 50,000 subscribers. However, because the system in *Scenario Two* uses filters, 35,000 customers have filters on their taps. Thus, an authorized subscriber in the *Scenario Two* system must remove a filter to gain access to the premium tier to use a pirate set-top or a pirate filter. Hence, *seventy percent* of the piracy among authorized subscribers is detectable. In *Scenario One*, system audits can only detect illegal drop-lines. *One hundred percent of the piracy among authorized subscribers is practically undetectable.*

Security Enhancement. The filters used in *Scenario Two* enhance the security provided by either set-top converters or positively secured channels. An authorized subscriber who removes the filters may receive unsecured commercial satellite channels on upper tiers but the subscriber will still not receive the channels secured with converters or a positive security system unless the subscriber has a pirate set-top or a pirate trap.

Limiting Piracy. It should be obvious that the tier-filters used in *Scenario Two* limit the extent to which undetected pirate-converters can be used on authorized drop-lines. Using the lowpass filtering principles developed in Chapter 7, it is possible to use filters to limit piracy even further.

Assume that the system outlined in Table 8.2 is designed like the system represented in Table 7.10 of Chapter 7. If a lowpass filtering arrangement is used, only third tier customers have access to enciphered fourth tier premium signals because the last tier filter is taken off on third-tier drop-lines. If all pay channels which depend upon set-top converters are placed at the top of the band in the fourth tier, it is possible to place a tier filter on all third tier drop-lines to block premium channels to all third customers who take only third channels. Hence, pirate converters will not work on third tier drop-lines. This reduces *undetectable* piracy from 50,000 drop-lines to only 5,000 drop-lines. But all of the customers on the fourth tier must purchase at least one premium channel and rent a set-top converter anyway. Assuming a piracy rate of twenty percent, the amount of undetectable piracy on the system would be twenty percent of 5,000 subscribers. *That is an absolute piracy rate of only two percent.*

Strategic War Planning

Using the methods developed in previous chapters, it is possible to formulate a strategic war plan against pirates which includes elements of physical security, communications security, psychological warfare, electronic counter measures, and legal prosecution. The plan could include the following elements -

1. tier filtering to reduce costs and increase the ability of the operator to detect piracy,

2. periodic tap audits to detect unauthorized drop-lines and missing traps,

3. use of a system design which allows the operator to implement a contingency plan to place tier-filters on all drop-lines which do not use set-top deciphering,

4. use of set-tops which can be disabled using a computer virus transmitted by the headend computer,

5. use of set-tops with "resilient" encryption systems based upon smart cards, and

6. implementation of an anti-piracy campaign when significant levels of piracy are detected.

With this type of carefully crafted strategic plan in place, it is possible monitor drop-line piracy using periodic audits. Note that filtering third tier drop-lines from the start is *not recommended.* Filtering third tier drop-lines should be *held in reserve* as a contingency plan for implementation at an appropriate time.

When significant use of modified or pirate set-top converters is detected in the system, an anti-piracy / amnesty campaign can be implemented followed by prosecution of pirates detected during audits. A computer virus can then be transmitted to all unauthorized set-tops. Next, lowpass filters can be placed on all third tier drop-lines. When third tier drop-lines are filtered, it is important to schedule a follow-up audit of third tier drop-lines six months after implementation. This will identify any additional pirates which were not previously identified. Finally, all smart cards in authorized converters can be replaced.

Like using antibiotics, it is important to use only those remedies which are necessary and sufficient to remedy the problem. In this way, remedies can be "held in reserve" for implementation unexpectedly if a piracy problem reoccurs.

Works Consulted

Mike Bates and Robert Depweg, "How Continental of LA Thwarted Complex Piracy-Ring" in ***Communications & Engineering Design.*** June 1994. pp. 58, 62, 60, 64.

Norm Bedoucha, "Piracy On The High Seas of Cable" in ***Communications Technology.*** November 1995. pp. 28, 30.

Guy Gugliotta and Jeff Leen, ***Kings of Cocaine***. New York, N.Y.: Harper & Rowe, 1990.

Linda Haugsted & Joe Estrella, "Cabletrap Jolts Ops On Piracy War" in ***Multichannel News***. May 12,1997, pp. 3, 16.

John Kerry, ***The New War: The Web of Crime That Threatens America's Security***. New York, N.Y.: Simon & Schuster, 1997.

Dy Rheu Kuston, Henry Schwoh, and Susphun Pagann, "Combatting Cable Signal Theft" in ***Communications & Engineering Design.*** June 1995. pp. 58, 60 - 63.

John Lamrande, "Building A Better Mousetrap" in ***Communications & Engineering Design.*** *June 1993. pp. 72, 74 77.*

Harry Maxwell, "Setting Up A Sting To Snag Cable Crooks" in ***Communications Engineering & Design***. June 1997. pp. 46 48, 50.

National Cable Television Association, ***Signal-Security Handbook: A Resource Manual for Cable-Operators.*** Washington , D.C.: National Cable Television Association, 1993.

National Cable Television Association and the Coalition to Oppose Signal-Theft, "Cable Theft Is A Crime: Education Kit [Loose-Leaf Folder]. Washington, D.C.: National Cable Television Association, nd.

Paul Paradise, "Signal-Theft" in ***Electronics Now.*** January 1995. pp. 33-40, 90.

Bill Rivas, "Jones Intercable's Theft of Cable Amnesty Program" in ***Communications & Engineering Design.*** June 1996. pp. 94, 96, 98, 99.

Kathleen Scoop, Barry Rosenblum, and Daniel J. Lefkowitz, "Time-Warner Cable NYC Attacks Theft At All Levels" in ***Communications & Engineering Design.*** June 1996. pp. 100, 102, 104.

United States Office of the Law Counsel of the House of Representatives, ***Title 18 United States Code Sections 1341 - 1346.*** Washington, D.C.: United States Government Printing Office, 1996.

United States Office of the Law Counsel of the House of Representatives, ***Title 18 United States Code Sections 1961 - 1968.*** Washington, D.C.: United States Government Printing Office, 1996.

United States Office of the Law Counsel of the House of Representatives, ***Title 47 United States Code Sections 553 - 605.*** Washington, D.C.: United States Government Printing Office, 1996.

Chapter 9
Tap Audits

No electronic program security system can effectively deter piracy without certain adjunct measures designed to identify and prosecute pirates. Such measures include physical security, cryptographic security, and tap auditing. When pay television filters are used in conjunction with such adjunct measures, tap audits can effectively identify two types of piracy - (1) drop-line piracy and (2) missing pay filters. However, because program piracy can include the use of illegal converters, a good tap auditing program should be part of a continuing and integrated anti-piracy campaign.

Classification

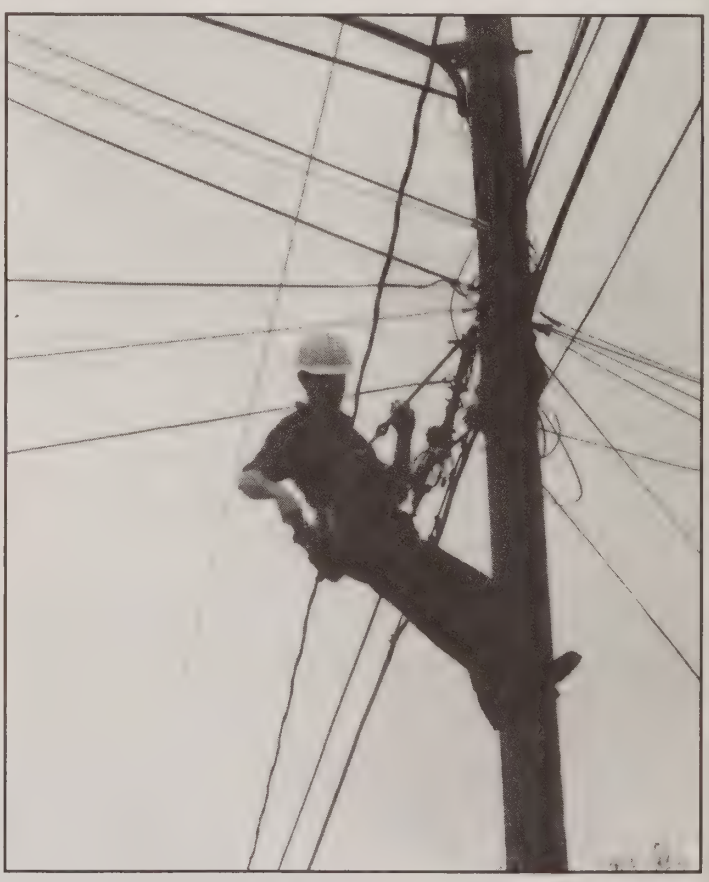
In general tap audits may be classified as either *procedural audits* or *special audits*. *Procedural audits* are conducted by service personnel during the regular course of business. By implementing a procedural audit program, a cable operator can turn most service calls into an opportunity to check nearby taps during installations and disconnects.

Special audits are conducted periodically to obtain a more accurate and systematic picture of the piracy situation within a specific franchise area. There are a variety of auditing firms for hire which will organize or carry out audits for cable operators. Special audits may be classified either by (1) method, (2) scope, or (3) geographical area.

In general there are two methods of auditing taps - (1) *ground audits,* and (2) *climbing audits*. *Ground audits* involve visually checking the status of taps and drop-lines from the ground. *Climbing audits* accomplish the same thing but the auditor actually climbs each pole to inspect tap connections more closely.

The scope of an audit depends upon its purpose. *Sample audits* are conducted using statistical procedures designed to estimate the piracy rate either within a specific franchise area or within some subdivision of that area. A *complete audit* is done when piracy rates are known to be high for the

Ground audits involve checking taps from the ground (Photo by C&E Corp.)



Climbing audits require a technician to actually climb a pole to inspect a tap (Photo by C&E Corp.)

AUDIT METHODS

Table 9.1

	Statistical	Complete
Ground Audit	Least Accurate	Relatively Accurate
Climbing Audit	Relatively Accurate	Most Accurate

purpose of identifying and prosecuting offenders.

Table 9.1 illustrates the relationship between these different classifications. While a statistical ground audit is less accurate than the other three special auditing methods, statistical ground audits are more accurate than non-random tracking statistics. They are also less expensive than any of the other three special auditing methods. Although a complete climbing audit will produce the most accurate results, it is also the most expensive method. Sample climbing audits and complete ground audits are relatively accurate but in different respects.

Auditing methods may also be classified as - (1) unblind, (2) blind, or (3) double-blind audits. Unblind audits are most efficient because the auditor carries a list giving him the status of taps. Only unauthorized taps are reported. With a blind audit the auditor is given the address of each tap but does not know what the status of each tap is supposed to be. He simply reports the level of service for each address. The reports are then matched with records at the office. Although this method is more cumbersome, it precludes "coffee shop" audits and assures that the work is really being done. With double-blind audits the auditor is not given either the address or the tap status. The auditor simply determines the status of each tap and reports the address to which it is connected.

Monitoring Strategy

It is possible to use the various auditing methods outlined above to identify and monitor piracy rates within a specific franchise area in order to identify problem areas and take remedial action before piracy gets out of hand. A *continuous tracking program* allows a cable operator to use field reports to formulate a geographic picture of piracy within a franchise area. *Special audits* of the whole area may be conducted periodically to obtain a more accurate picture of the problem. Alternatively, using the information gathered by a continuous tracking program, special audits may be conducted only within specific problem areas.

Piracy Detection Report

Technician:_____
Ward:____ **District:**____ **Date:**_____ **Time:**_____
Pole #_____ **Tap Assembly #**_____ **Tap:**_____
Street:_____
Name of Resident:_____

Type of Piracy:

[ ] **Unauthorized Drop-Line**
[ ] **Missing Tier Filter:**_____
[ ] **Missing Channel Trap:**_____
[ ] **Equipment Tampering:** [ ] **Tap**
[ ] **Line**
[ ] **Box**
[ ] **Set-Top Converter Tampering**
Set-Top #_____

Remarks:_____
_____
_____

Reporting, Enforcement, & Tracking

It is prudent for an operator to have a system in place for continuously monitoring piracy rates and enforcing anti-piracy laws. This involves three functions - (1) reporting by service personnel, (2) investigation of specific piracy reports, and (3) statistical analysis of piracy rates.

Reporting. System operators should establish specific procedures for reporting piracy. These procedures should include a special *piracy report form* for use by service personnel. Service personnel should be indoctrinated with respect to the need to report all piracy cases. Whenever a case of piracy is discovered in the field, service personnel *should not disturb the evidence*. Illegal drop-lines, splitters, or missing traps should be left in place for documentation by the *piracy enforcement bureau* or

the *security department*. Service personnel should complete a report form in duplicate. One copy of the form should go to the *enforcement officer* and another copy should be sent to the *analysis and tracking officer*.

Enforcement. Investigation of specific piracy cases is a *security function* which should be handled by someone with a background in law enforcement who is familiar with the procedure for gathering and documenting evidence. The *piracy enforcement officer* documents and investigates piracy cases. He or she should also work with the legal department and local law enforcement officials to prosecute piracy cases. For example, if service personnel have found sufficient evidence to establish *probable cause*, it may be possible for law enforcement authorities to obtain a search warrant based upon their affidavits.

Finding an unauthorized drop-line connected to a residence is not necessarily sufficient in itself to prove *legally* that the occupants of a residence connected the line or are using the service. To prosecute a case investigative personnel must prove certain *elements of larceny*. These elements include - (1) proving that a service was wrongfully taken, (2) proving ownership of the service, (3) proving the value of the service, and (4) proving that the accused *intended* to take the service illegally.[1] Proving intent is very important because no matter what the physical evidence shows, conviction depends upon intent. The NCTA's ***Signal Security Handbook*** outlines specific procedures for investigating piracy cases and gathering evidence.[2] It also contains procedures which make intent a lot easier to prove. The piracy officer may also run a telephone hot-line where subscribers may anonymously report piracy in their neighborhood. Unlike the analysis and tracking officer, the enforcement officer is primarily concerned with *specific cases*.

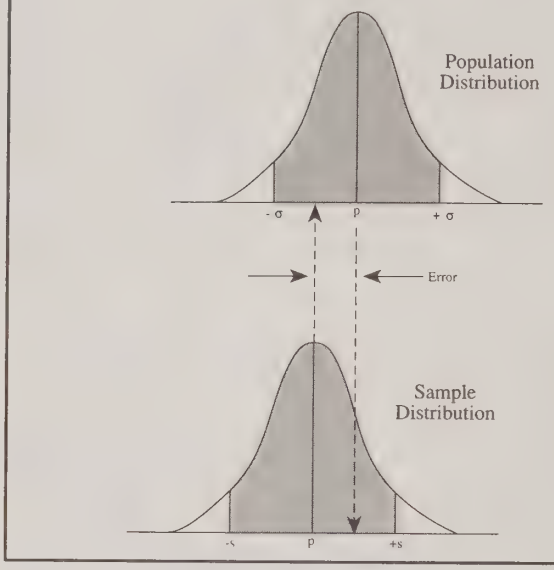
Analysis & Tracking. Analysis and tracking is a statistical *intelligence function* which involves

[1]Charles E. O'Hara, ***Fundamentals of Criminal Investigation.*** p. 348.

[2]National Cable Television Association, ***Signal Security Handbook: A Resource Manual for Cable Operators.***

POPULATION & SAMPLE DISTRIBUTION

Figure 9.1



representing the *aggregate piracy situation* for management. Such information is essential for formulating strategy and allocating resources to areas where resources will produce maximum results. Thus, the analysis and tracking officer is not at all concerned with specific cases except to the extent that they indicate future trends.

The analysis and tracking officer should be familiar with any statistical computer software used for analyzing statistical data. The officer should have at least one semester of *College Algebra* and two semesters of *Probability and Statistics*. The analysis and tracking officer compiles, summarizes, and reports periodic piracy rates within the franchise area. The officer also works with auditors during periodic tap surveys.

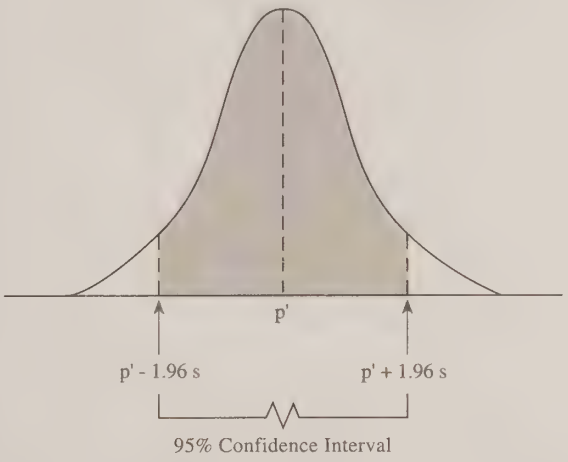
Statistical Methods

Using statistical methods it is possible to measure piracy rates and formulate a relatively accurate picture of piracy within a franchise area. Unlike grade point averages or demographic information, piracy rates must be handled statistically as "discrete variables." Just as one cannot be "half-pregnant," for analytical purposes either one has a case of piracy or one does not have a case of piracy.

The *sample piracy rate* (**p'**) measured by a random tap sample within an area may be calculated using the formula:

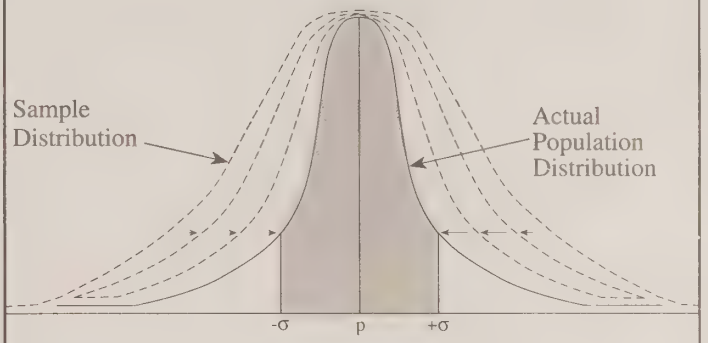
SAMPLE CONFIDENCE INTERVAL

Figure 9.2



SAMPLE ACCURACY

Figure 9.3



[1] $p' = 100 \times (x / n)$, where:

p' = the piracy rate (%),
x = the number of piracy cases in the sample, and
n = the number of taps sampled.

The *actual piracy rate* (**p**) which would result from a complete census of all taps within a specific area may be calculated using the formula:

[2] $p = 100 (x_t / n_t)$, where:

p = the actual piracy rate (%),
x_t = the actual number of piracy cases within the area, and
n_t = the number of taps within the area.

The values calculated using formulas [1] and [2] may be represented as either percentages (multiplying the ratios by one-hundred) or decimals.

According to *probability theory*, as the size of a random sample (**n**) approaches the size of a particular population (n_t), the value of the *sample piracy rate* (**p'**) will approach the value of the *actual piracy rate* (**p**). However, for practical purposes using "*large sample methods*" a *random sample* of between 500 and 1,600 can adequately represent almost any size population.[3] Beyond a certain point, increasing the size of a sample will not appreciably increase the accuracy of the estimate.

The standard deviation of a *binomial distribution* may be calculated using the formula:

[3] $\sigma = (p q / n_t)^{1/2}$, where:

σ = the standard deviation of the population,
$p = x_t / n_t$ = the decimal piracy rate,
q = (1 - p), and
n = the number of taps in the population.

When the standard deviation of a particular population is not known, it may be estimated using the standard deviation of the sample by substituting *p'* for **p** and letting $n = n_t$:

[4] $s = (p' q / n)^{1/2}$, where:

s = the standard deviation of the sample,
p' = x / n = the sample piracy (decimal) rate,

[3]David S. Moore and George P. McCabe, ***Introduction to the Practice of Statistics,*** pp. 588-89 and Paul G. Hoel, ***Elementary Statistics.*** p. 163.

q = (1 - p), and
n = the number of taps in the sample.

Figure 9.1 illustrates the relationship between the real distribution of a population and the distribution of a statistical sample. The 95-percent confidence interval around any particular statistical sample, illustrated in Figure 9.2, may be calculated using the formula:

[5] **e = p' +/- (z s)**, where:

e = the error of the estimate,
p' = x / n,
s = the standard deviation of the sample distribution, and
z = the statistical 'z' value corresponding to the desired level of confidence.

Using "*large sample methods*," the standard deviation of the sample (**s**) will approximate the standard deviation of the actual distribution (σ).

For a 95-percent confidence interval, a "**z** value" of 1.96 is used. Thus, the 95-percent confidence interval for a distribution may be calculated as **p' +/- 1.96s**. In other words, given the 95-percent confidence interval for a random statistical sample, one can be 95-percent certain that the actual piracy rate (**p**) lays within the confidence interval. Alternatively, there is only a 5-percent chance that the real piracy rate lays outside the confidence interval.

As the size of the statistical sample increases, the standard deviation of the sample becomes narrower. Thus, the confidence interval becomes narrower. Consequently, as the size of statistical sample increases, the accuracy of the estimated piracy rate (**p'**) increases. However, as previously indicated, there is a point of diminishing returns beyond which increasing the sample size will not significantly increase the accuracy of an estimate.

Procedural Audits

Procedural audits provide cable operators with a continuing flow of information concerning piracy within a specific franchise area. Reports by service personnel may be compiled on a monthly basis to calculate piracy rates for the entire franchise area and for particular subdivisions of the franchise area. However, because the reports are *not* collected using random sampling methods, the results obtained will *necessarily be less accurate and less certain than results obtained from a strictly random sample*. In particular, because some districts may have a greater turn-over rate, the number of service calls within the area may not proportionally represent the area properly in relation to the entire system. Further, since the process through which taps are audited is not purely random, the reliability of the sample will be questionable. Nevertheless, the data gathered during procedural audits can be useful in that it will tend to reflect what is going on.

Data collected and reported by installers during routine work may be used to produce three different kinds of reports. First, reports can be used to estimate piracy rates within the franchise area. Second, the reports may be *cross tabulated* to determine what kind of piracy is most common in various parts of the franchise area. Third, the reports may be used to produce a *time-series analysis* of piracy both within specific districts and for the system as a whole.

A variety of computer software is made to calculate statistical parameters. In particular, *Anderson-Bell's* ***ABstat*** software is especially designed for processing statistical data. *Anderson-Bell's* ***ABsurv*** is especially designed for processing

Software Suppliers

Anderson-Bell Corporation
P.O. Box 5160
Arvada, CO 80005
Phone: 1-800-745-9751
Fax: 1-303-940-0595

Lotus Development Corporation
55 Cambridge Parkway
Cambridge, MA 02142
Phone: 1-800-343-5414
Fax: 1-617-693-3899

Backdoor Group Inc.
10500 North Port Washington Rd. #107
Meguan, Wisconsin 53092
Phone: 414-241-3037
Fax: 414-241-3125

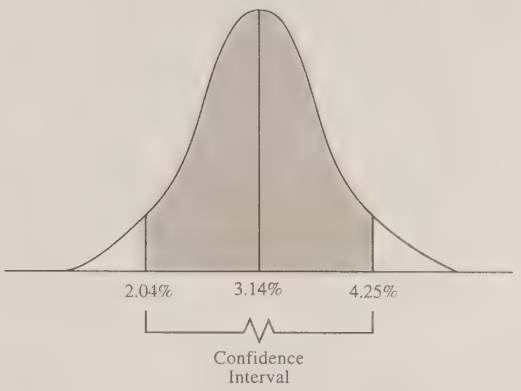
MONTHLY PIRACY RATES

Table 9.2

Ward	Piracy Cases	Total Dispatches	Piracy Rate (%)
1	11	203	5.42
2	5	351	1.42
3	7	196	3.57
4	7	205	3.41
Total:	30	955	3.14

CONFIDENCE INTERVAL

Figure 9.4



survey data. Both packages will calculate all of the statistical parameters commonly used to analyze statistical data. ***Lotus Spreadsheet*** is an excellent software package for doing cross tabulations. *Backdoor Group Inc.* offers a fully automated computer system for doing tap audits.[4]

Mean Piracy Rates. In order to estimate the average or mean piracy rate from field reports one must have two pieces of information - (1) the number of monthly piracy cases reported within a specific area, and (2) the number of monthly dispatches within the same area. Hence, the service department must keep track of monthly dispatches within each district and turn in a copy of each piracy report. Table 9.2 illustrates how this data may be summarized. Using formulas [4] the overall standard deviation may be calculated for the whole system:

[6] $\mathbf{s = [(0.0314 (1 - 0.0314)) / 955]^{1/2} = \cong 0.005645}$

Using the standard deviation with formula [5], the 95-percent confidence interval for the distribution may be calculated as:

[7] $\mathbf{0.0314 +/- 1.96 (0.005645) = 0.0314 +/- 0.0111 \cong 0.0203 \text{ and } 0.0425 = 2.04\ \% \text{ and } 4.25\ \%}$

Figure 9.4 illustrates this confidence interval around the sample mean of 3.14-percent. Thus, if the statistical sample were purely random, the probability would be 95-percent that the actual piracy rate falls within the confidence interval between 2.04-percent and 4.25-percent. Because the estimated piracy rate in *Ward 1* is outside the 95-percent confidence interval, the piracy rate in *Ward 1* appears to be significantly different from the overall piracy rate.[5] This could indicate significantly higher piracy rates in Ward 1.

Since the data was not collected using a *purely random statistical sample*, such estimates are *not statistically valid.* Because of the way in which the data was collected, there is no assurance that the samples from particular wards proportionally represent the tap population within those areas. Nevertheless, to the extent that random influences are operating in the collection process such estimates may provide some indication of what is occurring within a particular franchise area. When this kind of information is used with a periodic statistical audit of the entire franchise area, it is possible to obtain more accurate *statistically valid estimates.*

Cross Tabulation. The data derived from procedural audits may be compiled and cross tabulated, as shown in Table 9.3, to derive

[4]Cf. Kenneth Higgins, "Closing the Backdoor On Signal Theft" in ***CED***. June 1997.

[5]More sophisticated and reliable tests are available for testing whether two means are statistically different. Most statistical software packages include provisions for doing t-tests and hypothesis testing.

CROSS TABULATION

Table 9.3

Basic Data

Ward	Drop Line	Converter Tampering	Missing Channel Trap	Missing Tier Traps One	Missing Tier Traps Two	Total
1	3	2	3	4	2	14
2	2	1	1	2	2	8
3	1	2	1	2	1	7
4	4	3	6	4	3	20
Totals:	10	8	11	12	8	49

Row Percentages

Ward	Drop Line	Converter Tampering	Missing Channel Trap	Missing Tier Trap One	Missing Tier Trap Two	Totals
1	21.43	14.28	21.43	28.57	14.28	100.00
2	25.00	12.50	12.50	25.00	25.00	100.00
3	14.29	28.57	14.29	28.57	14.29	100.00
4	20.00	15.00	30.00	20.00	15.00	100.00
Totals:	20.41	16.32	22.45	24.49	16.32	100.00

Column Percentages

Ward	Drop Line	Converter Tampering	Missing Channel Trap	Missing Tier Traps One	Missing Tier Traps Two	Total
1	30.00	25.00	27.24	33.33	25.00	28.57
2	20.00	12.50	9.10	16.67	25.00	16.33
3	10.00	25.00	9.10	16.67	12.50	14.29
4	40.00	37.59	54.56	33.33	37.75	40.82
Totals:	100.00	100.00	100.00	100.00	100.00	100.00

Composite Percentages

Ward	Drop Line	Converter Tampering	Missing Channel Trap	Missing Tier Traps One	Missing Tier Traps Two	Total
1	6.12	4.08	6.12	8.16	4.08	28.57
2	4.08	2.04	9.09	4.08	4.08	16.33
3	2.04	4.08	9.09	4.08	2.41	14.29
4	8.16	6.12	12.25	8.16	6.12	40.82
Totals:	20.41	16.33	22.45	24.49	16.33	100.00

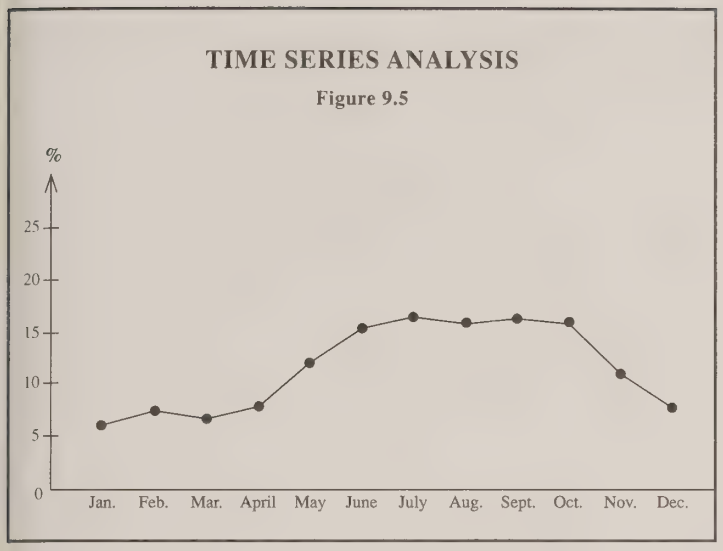
information concerning the composition of the sample. *Cross tabulation* is a powerful statistical method used for uncovering patterns in a statistical sample. By calculating column percentages it is possible to determine where the majority of the piracy cases within any particular category were found. By calculating row percentages, it is possible to determine the composition of the piracy cases within any particular ward. Finally, by calculating percentages based upon the sum total, it is possible to determine whether most of the piracy within a particular category is occurring within a particular area or whether the rates are fairly uniform throughout the franchise area.

Table 9.3 illustrates some specific examples. The composite percentages in Table 9.3 show that 40.82-percent of the piracy in the system occurs within Ward 4. The column percentages show that more than half of the channel trap piracy in the system occurs in Ward 4. The row percentages show the composition of the piracy within Ward 4.

Time-Series Analysis. If monthly data is graphed in relation to time, it is possible to produce a time-series which *tracks particular piracy categories over time.* Piracy rates may be graphed in relation to time to show trends. This may be done either for the whole system or for particular wards or districts within the system. Such data is useful for measuring seasonal trends, determining whether rates are increasing or decreasing, and determining whether anti-piracy campaigns are producing measurable results.

Special Audits

Special audits are used for measuring piracy rates with greater precision. A complete audit involves a complete census of all taps either from the ground or by climbing each pole. Because a complete audit of an entire franchise area can be expensive, usually an entire franchise area is not audited unless *piracy is rampant throughout the entire system.* Continuous monitoring is designed to avoid this kind of situation. Statistical audits represent a way of accurately



determining piracy rates without actually doing a census of the whole system. It is then possible to identify specific wards or districts where piracy rates are high in order to do a complete audit in those areas.

A statistical audit is done by randomly sampling taps throughout a specific area. This can be done within a franchise area by assigning each tap assembly in the system a number. For example, if a system has 9,000 tap assemblies, the assemblies would be numbered as 1 to 9,000. Assuming eight taps on each tap assembly, this would represent a total of 72,000 taps. If one selected every 34th assembly one would draw *a cross sectional sample* of the entire system. Further, since the sample is random, it will have all of the properties of the original population. One can *randomize* the sample by simply selecting a random number between one and thirty to use as the number of the first tap assembly. Hence, if one selected the number eleven at random, one would start with Assembly Number 11 and check every 34th assembly. The tap assembly numbers could be generated using the formula:

[8] $\mathbf{f(x) = R + 34\,(n - 1)}$, where:

R = a random starting number between one and thirty, and
n = 1, 2, 3, ...250

Thus, the first four assembly numbers would be 11, 45, 79, 113, 147, etc., up to assembly number 8,477. Assuming eight taps on each assembly, the total sample would represent 2,000 taps.

For practical purposes, the *business management computer* can be programmed to generate the sample giving the location of each tap. If twenty installers are each assigned twelve or thirteen assemblies to check, the entire sample could be collected in a single day. It is desirable to have a random survey sample collected as quickly as possible so that it represents a statistical "snap shot" of the original population. If the sample is collected over an extended period of time, the properties of the population may change during the survey. This will adversely affect the accuracy of the statistical measurements.

The reports from the sample audit are compiled and processed using statistical software as illustrated in the previous examples using formulas [1], [4], and [5]. If all of the raw data from the survey sample is entered into a computer file, the file itself will represent a statistical model of the survey area. Such a model can be very useful to a specialist with advanced research training for checking a variety of the theories or hypotheses. The sample data may also be cross tabulated to look at the composition of the sample. Thus, the sample audit can be compared with the information from continuing procedural audits to decide which areas require more detailed attention. Once the high piracy areas within the franchise area have been identified complete audits can be done in those areas.

Works Consulted

Anderson-Bell Corporation, ***ABStat.*** Arvada, Colorado: Anderson-Bell Corporation, 1987.

Anderson-Bell Corporation, ***ABSurv.*** Arvada, Colorado: Anderson-Bell Corporation, 1991.

Mike Bates and Robert Depweg, "How Continental of LA Thwarted Complex Piracy Ring" in ***Communications & Engineering Design.*** June 1994. pp. 58, 62, 60, 64.

Allen L. Edwards, ***Statistical Methods for the Social Sciences.*** New York: Holt, Rinehart, and Winston, 1962.

Kenneth Higgins, "Closing the Back Door on Signal Theft" in ***Communications & Engineering Design***. June 1997. pp. 52, 54 56, 58, 60.

Paul G. Hoel, ***Elementary Statistics.*** 4th Edition. New York: John Wiley & Sons, Inc., 1976, p. 163.

Dy Rheu Kuston, Henry Schwoh, and Susphun Pagann, "Combatting Cable Signal Theft" in ***Communications & Engineering Design.*** June 1995. pp. 58, 60 - 63.

John Lamrande, "Building A Better Mousetrap" in ***Communications & Engineering Design.*** *June 1993. pp. 72, 74, 77.*

Lotus Development Corporation, ***Lotus Spreadsheet.*** Cambridge, MA: Lotus Development Corporation, 1989.

Harry Maxwell, "Setting Up A Sting To Snag Cable Crooks" in ***Communications & Engineering Design***. June 1997. pp. 46 48, 50

David S. Moore and George P. McCabe, ***Introduction to the Practice of Statistics.*** New York: W.H. Freeman and Company, 1989.

National Cable Television Association, ***Signal Security Handbook: A Resource Manual for Cable Operators.*** Washington , D.C.: National Cable Television Association, 1993.

National Cable Television Association and the Coalition to Oppose Signal Theft, "Cable Theft Is A Crime: Education Kit [Loose Leaf Folder]." Washington, D.C.: National Cable Television Association, nd.

Charles E. O'Hara, ***Fundamentals of Criminal Investigation.*** 4th Edition. Springfield, Ill.: Charles C. Thomas, 1976.

Bill Rivas, "Jones Intercable's Theft of Cable Amnesty Program" in ***Communications & Engineering Design.*** June 1996. pp. 94, 96, 98, 99.

Kathleen Scoop, Barry Rosenblum, and Daniel J. Lefkowitz, "Time-Warner Cable NYC Attacks Theft At All Levels" in ***Communications & Engineering Design.*** June 1996. pp. 100, 102, 104.

Chapter 10
Physical Security

A sound physical security program is essential to preserving the security of pay television programming. To accomplish that objective, a variety of physical security provisions are necessary. These provisions include - (1) tap security, (2) converter security, (3) building and vehicle security, (4) internal and external controls, and (4) computer security.

Tap Security

Physical security begins by securing all taps, pole boxes, and curb pedestals. When taps are located on overhead lines, a ladder is required to reach them. However, sometimes lines are run underground. In that case taps must be located in curb pedestals. In large apartment buildings taps are occasionally located in locked boxes located on the side of the building.

Lock boxes, curb pedestals, or other equipment enclosures may be secured using a variety of locks or special security screws. Warning labels may also be used on equipment enclosures to notify potential vandals of criminal penalties. Overhead taps are usually secured using "security sleeves" or "shields."

Security Shields. Most if not all filter manufacturers make "security shields" or "tap sleeves" in several different sizes for locking filters, terminators, or drop lines onto taps. They fit over the filters, terminators, or drop-line connectors to prevent unauthorized personnel from tampering with them.

TYPICAL SECURITY SHIELD
Cross Sectional Diagram

Figure 10.1

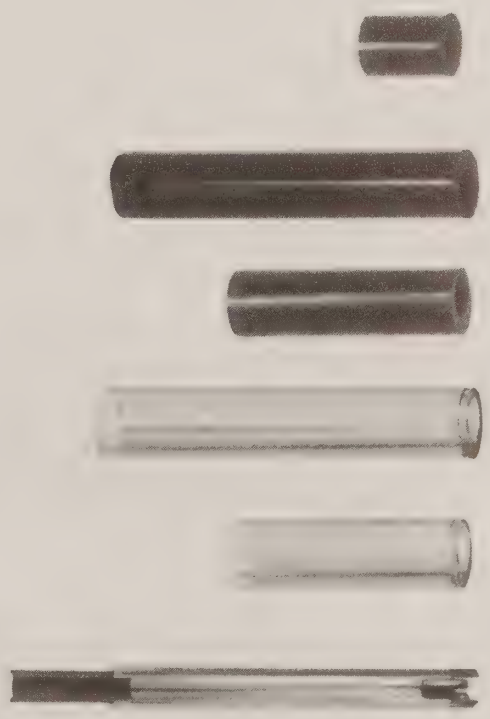
Tap shields are usually made of molded black ABS plastic or clear "lexan" plastic. One inch shields are used for locking drop-line connectors and terminators. Four or six inch shields are used for locking filters.

A special connector tool is used for attaching or removing the shields. One end of the tool is used for locking or unlocking F-connectors and the other end is used for installing or removing filters. Figure 10.1 illustrates a cross section of a typical security shield. The interior of the sleeve is round to fit over a cylindrical filter. The exterior shape of the sleeve is elliptical to restrict rotation. Thus, the sleeve cannot be removed without using the proper tool.

Multi-color overlay labels are made for use with clear shields to assist with visual auditing from the ground. Specific color codes may be used to indicate the status of various taps. Typical classifications include - (1) active, (2) disconnected, (3) a specific tiers, or (5) a specific premium channel.

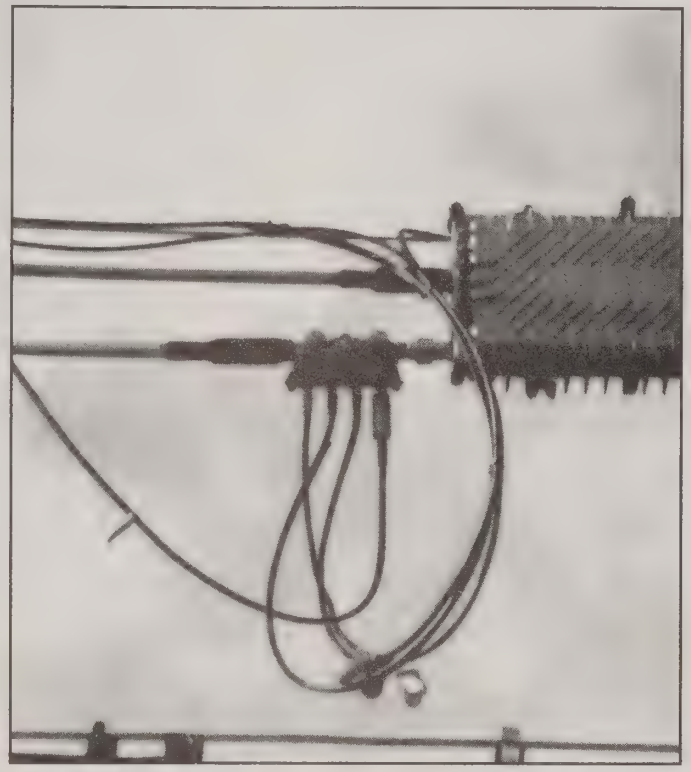
Locks. Locks can be useful for securing pedestals and pole boxes. Although most locks can be broken or defeated, a simple lock can complicate life for a cable pirate. Locks slow down a pirate's work and

TYPICAL SECURITY SHIELDS & TOOLS
(Courtesy of Arcom CATV Products)



TAP SECURITY

(Photos by C&E Corp.)



Overhead Taps

Curb Pedestal

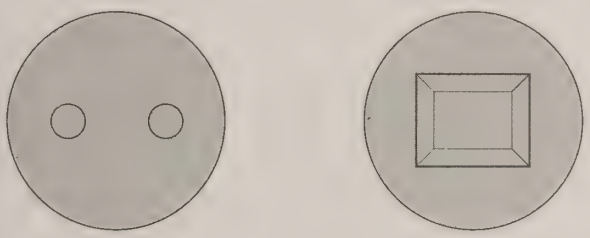
Lawn Pedestal

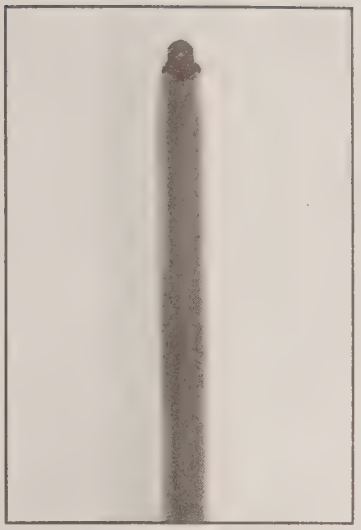
Lock Box

The physical security of the distribution network is an essential element of program security.

TYPICAL SECURITY SCREW HEADS

Figure 10.2





Special screwdriver heads on typical security screw tools (Photo by C & E Corp.)

make criminal activity more obvious to observers. Locks also have *a significant legal role in prosecutions*. One of the *elements of proof* in larceny cases involves *proving intent*. In court, it is more difficult to argue that something of value was taken if the owner did not bother to secure it with a lock. On the other hand, it is difficult for a vandal to argue "*lack of intent*" if a lock was broken. A wide variety of locks and locking devices are made for almost every piece of equipment imaginable.

Security Screws. A variety of special security hardware, made for use with security alarm systems, can be used by cable operators for securing equipment, pole boxes, and curb pedestals. Such hardware includes a variety of special security screws. Security screws require a screwdriver with a special head to insert or remove them. So-called "snake-eye" screws are made in a variety of different sizes. Some other types of security screws require a screwdriver with a square head of a specific size.

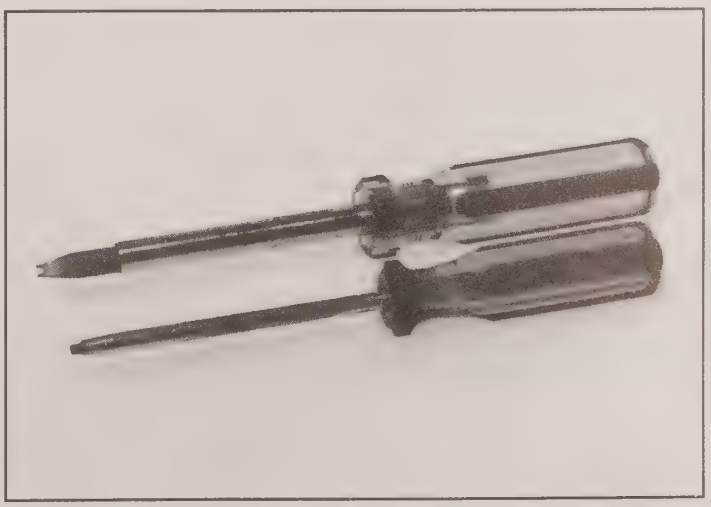
Warning Labels. Placing warning labels on locked equipment, pole boxes, and curb pedestals citing relevant larceny statutes can help deter pirates from tampering with equipment. The labels should cite the relevant statute and the maximum penalty for violating the statute. A statement should also be included on the label that violators will be prosecuted to the full extent of the law.

Even if tampering occurs, warning labels help prosecutors make convictions. By placing a warning label on every piece of equipment which might be of interest to a pirate, a cable operator can make it easier for authorities to establish the *culprit's intent*. It is harder for a pirate who ignored a warning and broke a lock to argue "*lack of intent*."

Set-Top Security

Because set-top converters are in the customer's home, they are very vulnerable to tampering. Although it is almost impossible to design a tamper proof set-top converter, it is possible to make converter tampering more difficult and more detectable.

One way of making converter tampering more difficult is to *replace important screws on the set-top with either "snake-eye" screws* or some other security screws. Special *self-adhesive security stickers* are made for placing over important screws. Such stickers are printed on very tacky backing which



Typical screwdrivers for special security screws (Photo by C & E Corp.)

Since equipment can be stolen from warehouse stocks, building security is an essential part of program security (Photo by C&E Corp.).

makes any tampering immediately evident. Use of specially marked *stickers* over important screws can make set-top tampering more detectable. These steps are particularly important if an operator takes the risk of losing positive traps by placing them inside set-top converters.

Buildings & Vehicles

The physical security precautions taken to protect the security of programming should not be limited to taps, pole boxes, curb pedestals and set-top converters. Warehouse security and vehicle security are equally important. It is not uncommon for certain pirate installers to use equipment stolen from the cable operator. It more difficult to identify unauthorized drops if pirate installers are using the same equipment as the cable operator.

Access to stocks of *security tools*, *set-top converters*, and *positive traps* should be limited within the warehouse to only authorized employees. Sensitive items should be stored in areas which are

Since equipment can be stolen from vehicles, vehicle security is an essential part of program security (Photo by C&E Corp.).

"compartmented" from less sensitive supplies. In order to limit the possibility of employee theft, unauthorized employees should not be allowed free access to sensitive equipment or sensitive tools.

It is equally important to assure that unoccupied vehicles in the field are secure while crews are working on poles or in homes. Employees should be reminded to lock their vehicles while they are working. In addition, vehicles should contain a separate locked box or bay for carrying converters and positive traps.

Internal & External Controls

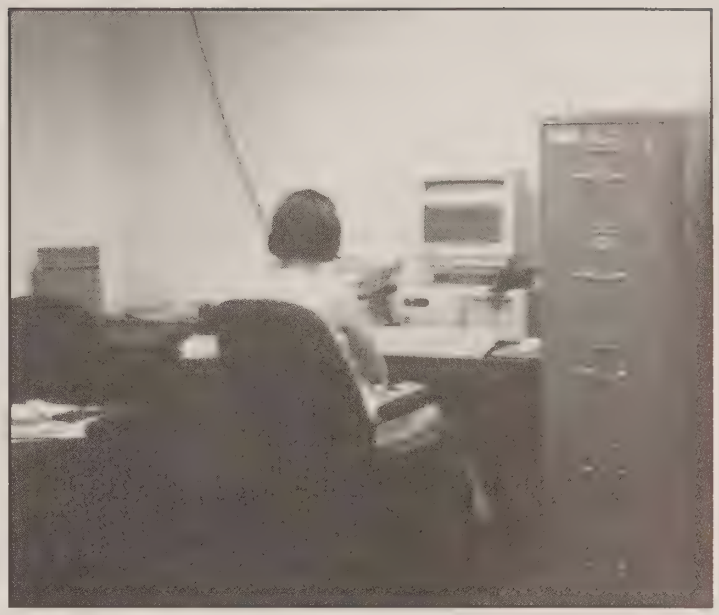
Appropriate accounting, auditing, and inventory control procedures should be implemented to preserve the physical security precautions taken by the operator. Just as tap audits help detect drop-line piracy, a good quality control program can help detect a variety of *employee schemes* to sell stolen equipment or services.

Quality Control. A quality control program can be implemented by having a quality control technician check jobs after the they are complete. Installer names may be selected at random from a pool each day. The quality control technician then checks a sample of the selected technicians' work. If disconnects are not are being performed, the problem will be detected.

Only certain employees should be permitted access to stocks of positive traps (Photo by C&E Corp.).

Inventory Control. Accounting, auditing, and inventory control procedures can determine whether tools or equipment are being stolen from inventories. Receipts should be required for *all sensitive tools and equipment* at the time they are issued to installers. The installer should obtain receipts for set-top converters from the customer acknowledging the customer's responsibility for return of the converter. By implementing internal control procedures it is possible to *trace the disposition* of every piece of sensitive equipment in the system. Such internal controls can also help isolate "where" losses are occurring.

By "compartmenting" sensitive supplies and implementing proper control procedures it is possible to isolate where losses are occurring. For example, suppose one thousand positive traps were received at the warehouse for stock. If five hundred were used for installations but only four hundred fifty show up on the inventory one can conclude that traps are missing from inventory. If no defective traps were returned and only a limited number of personnel had access to stocks, the list of possible suspects is



Files in the Business Management Computer and the System Central Computer should be protected with passwords (Photo by C&E Corp.).

limited to only those individuals who had access to stocks. Investigation can then focus on *those people* and in *that area*.

Compartmentalization. Program piracy has become a "racket" involving organized crime. It is "big business" and many of the criminal organizations involved in it have access to considerable sums of money. In some instances, there have been attempts to bribe employees in order to gain access to restricted information.[1] Hence, manufacturers and cable operations are potential *espionage* targets.

Long ago, the intelligence and national security community developed procedures for dealing with such problems. The concepts of *compartmentalization* and a *"need to know"* are used to limit access to sensitive information and materials. Thus, the government classifies information as either "confidential," "secret," or "top secret" according to the level of harm which revelation would cause to national security. However, security procedures do not stop with security clearances and classifications. A security clearance does not automatically give cleared personnel unrestricted access to sensitive

[1]Linda Haugsted and Joe Estrella, "Cabletrap Jolts Ops On Piracy War" in ***Multichannel News.*** May 12, 1997, pp. 3, 10. Cf. Senator John Kerry, ***The New War.***

information even if the personnel are trustworthy. Within each security classification information is *subclassified* using a variety of *"special accesses."* Thus, regardless of one's rank or security clearance personnel are not permitted access to compartmentalized information or materials unless they have a bonafide "need to know." In this way the risk of compromising sensitive information is limited to an absolute minimum.

The concepts of compartmentalization and a "need to know" can be used by manufacturers and cable operators to limit the risk of losing sensitive equipment or information. This can be done by establishing at least three levels of access which seperates the public from employees and employees from personnel with a bonafide need for access. For example, a computer operator with a bonafide need for access to encryption keys does not necessarily have a bonafide need for access to stocks of set-top converters. Similarly, installation personnel with a bonafide need for access to set-top converters may not necessarily have a bonafide *need to know* the encryption keys used.

Compartmentalization also assists investigators in identifying the source of "leaks" since the knowledge of leaked information is limited to a specific population. It is even possible for investigators to plant unique information within a specific compartmented population in order to trace the source of suspected leaks. Such techniques are often useful in tying a felon to a criminal conspiracy under the RICO statutes.

Computer Security

Precautions should be taken to ensure the physical security of the *business management computer* (BMC) and the *system control computer* (SCC). Software used for generating any *cryptographic keys* should be *protected by passwords* so that only authorized personnel have access to sensitive computer files. It is equally important to *limit access to customer records* so that records cannot be changed or modified by unauthorized personnel.

Employee Screening

All security programs depend upon the integrity of the employees who carry them out. Certain employees should be screened when they are hired. Proper screening will not only enhance a system's security program but it will also help *protect customers*.

Employee screening begins by asking all employment applicants whether they have ever been *convicted* of either a misdemeanor or a felony. Applicants should also be asked to sign an information *release form* so that names can be checked with the police. This is particularly important in *large urban systems* which have a large number of employees.

Although it is *not necessary to run name checks on all applicants,* applicants for certain jobs should b checked. These include installers, warehouse personnel, and computer personnel with access to

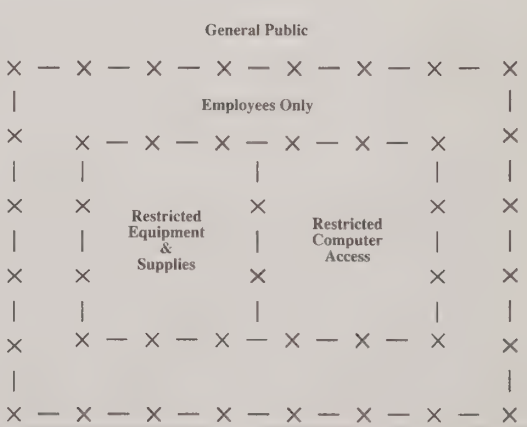
CLASSIFICATION VS. ACCESS

Figure 10.3

	Access Examples		
	Crypto	Specat	SIOP
Confidential			
Secret			
Top Secret			

COMPARTMENTALIZATION

Figure 10.4



customer records. Convictions for *larceny, burglary, robbery, driving while intoxicated, or substance abuse* are offenses which should be considered in hiring.

The *records division* of all Police Departments maintains a list of criminal convictions. Police also have access to a variety of national crime reporting networks. With signed release forms, the names of applicants can be checked by the Police for criminal convictions. Usually there is a nominal fee for name checks of between $ 5.00 and $ 10.00 per name.

Works Consulted

Edward W. Cleary, ed., ***McCormick's Handbook of the Law of Evidence***. 2nd Edition, St. Paul, Minn.: West Publishing, 1978.

Guy Gugliotta and Jeff Leen, ***Kings of Cocaine***. New York, N.Y.: Harper & Row, 1990.

Linda Haugsted and Joe Estrella, "Cabletraps Jolts Ops On Piracy War" in ***Multichannel News***. May 12,1997, pp. 3, 10.

John Kerry, ***The New War: The Web of Crime That Threatens America's Security***. New York, N.Y.: Simon & Schuster, 1997.

Graham C. Lilly, ***An Introduction to the Law of Evidence***. St. Paul, Minn.: West Publishing, 1978.

National Cable Television Association, ***Signal Security Handbook: A Resource Manual for Cable Operators.*** Washington, D.C.: National Cable Television Association, 1993.

National Cable Television Association and the Coalition to Dipore Signal Theft, "Cable Theft Is A Crime: Education Kit [Loose Leaf Folder]. Washington, D.C.: National Cable Television Association, nd.

Charles E. O'Hara, **Fundamentals of Criminal Investigation**. 5th edition. Springfield, Illinois: Charles C. Thomas, 1976

Chapter 11
Cryptographic Systems

Although pay television filtering can reduce piracy levels and make piracy more detectable, most if not all cable operators must use set-top converters or addressable taps with filters for customers who subscribe to a lot of premium channels. It has been observed that *all program encryption systems are vulnerable to analysis*. While most subscribers are not cryptanalysts, there are "hackers," pirate distributors, and elements of organized crime which have sufficient resources to duplicate almost anything. Thus, it is obviously desirable to use the most secure cipher system available. Hence, the question arises: *What characteristics or properties make a cipher system more secure? This question can be answered by cryptology.*

Properties Of A Good Cipher System

Cryptology is defined as the art and science of making and breaking ciphers. Cryptology is sometimes considered one of the "black arts" because much of the field has traditionally been practiced in secret. For this reason, most people don't know much about it. As a field, cryptology is divided into two areas - (1) *cryptanalysis*, and (2) *cryptography*. *Cryptanalysis* is the art and science of breaking ciphers while *cryptography* is the art and science of making them. The word "*cryptography*" is derived from greek and literally means "*hidden writing.*" As a field cryptography is more than two thousand years old. As a well established field of study, cryptography *has certain well established conventions, definitions, and principles.*

It has been observed that cipher systems are very "fragile." Like a chain, *a cipher system is only as strong as its weakest link.* The properties of a good cipher system are listed in Table 11.1. A failure to meet *any one of these properties* is a *fatal flaw* - sufficient to make the system vulnerable to analysis and compromise.

For a variety of reasons, cipher systems are not well suited to protecting premium television programming. Properties 7, 8, 9, 12, and 13 (*) are inconsistent with practical program security requirements. For example, it is not practical to send each subscriber a daily key by courier or mail. Even sending a monthly key would be expensive.

The security of *both the key and the plain text* are equally important for protecting the security of each.

PROPERTIES OF A GOOD CIPHER SYSTEM

Table 11.1

1. *The cipher system should be designed so that compromise of the cipher equipment will not compromise the cipher system itself.*
2. *The cipher system should be resistant to "frequency analysis" or character/symbol counts which allow deduction of the most frequent symbols or characters.*
3. *The cipher system should have sufficient "key depth" to assure that the key stream will never repeat within a message.*
4. *The cipher system should have a sufficient number of daily keys to preclude testing every possible key using special purpose computers operated in parallel at a speed much higher than the fastest available computers.*
5. *The cipher system should be designed so that the key stream is never "exposed" when there is no program input.*
6. *Master keys should be totally random.*
7. *Master keys should be changed daily.**
8. *Master keys should never be sent over a communications link even if the link itself is enciphered.**
9. *Master keys should be sent via mail or courier.**
10. *Each message should use a unique and random "session key" which is not reused again.*
11. *Each communications link in a network should use a unique and random "session key" which is not duplicated in any other link.*
12. *Keys must be kept secret.**
13. *Plain text must be kept secret.**
14. *The cipher system should be designed so that it does not propagate errors if one piece of data is misread.*

Knowledge of either will compromise the other. Cipher systems *assume* the integrity of the recipient user. In pay television *any subscriber* could be a pirate or an illegal distributor. Thus, to insure security the key itself must be *kept secret from the recipient user.* This is *practically impossible* since someone will eventually figure out how to read the keys being used by their equipment no matter what the form. It is equally impossible to sell a program *publicly* while still keeping it "secret." Whenever the "plain text" program is publicly available, it is possible to deduce the key.

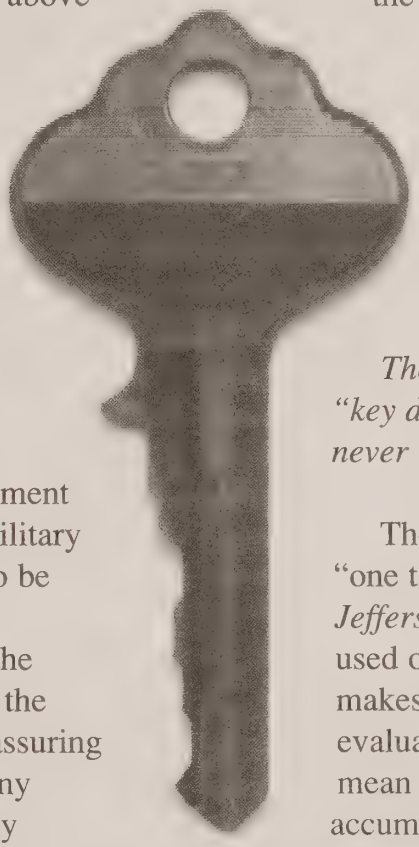
Rationale

Each of the properties recommended above are based upon the actual experience of cryptographers and cryptanalysts.

The system should be designed so that compromise of the cipher equipment will not compromise the cipher system itself.

Despite their efforts to keep cryptographic equipment out of enemy hands, military planners assume that sooner or later their cryptographic equipment will be captured by the enemy. Thus, military cryptographic algorithms are designed to be independent of the equipment so that compromise of either the equipment or the equipment designs will not compromise the cryptographic system. This is done by assuring that the cryptographic system has so many possible keys that decryption is not likely without the specific key used to encrypt particular messages.

This requirement is very close to the requirements of the pay television industry where any subscriber can be a pirate. Despite such design features, in practice, compromise of crypto equipment can help a cyptanalyst break a cipher system by allowing the analyst to evaluate the equipment for flaws and idiosyncrasies.



The cipher system should be resistant to "frequency analysis" or character/symbol counts which allow the deduction of the most common characters/symbols.

Every language has certain vowels which tend to occur more frequently than other letters in the alphabet. Audio and television pictures have similar characteristics. One way cryptanalysts break a cipher is to do a frequency count of each symbol in the cipher text. The most frequent letter occurring in the cipher text can be assumed to be the most frequent letter in the language being transmitted. Hence, frequency counts sometimes allow analysts to deduce certain parts of the message without having the key.

Cipher systems exist in which the frequency of symbols in the cipher text bears no relation to the symbol frequencies in the plain text. Such a system is said to be resistant to frequency counts.

The cipher system should have sufficient "key depth" to assure that the key stream never repeats within a single message.

The most secure cipher possible is called a "one time code." It was invented by *Thomas Jefferson.* With a one time code, a code is used only once and never used again. This makes it very difficult for an analyst to evaluate the code because each code could mean anything. The analyst cannot accumulate a meaningful history for analysis. Further, even if a one time code is compromised it yields no information about future codes. Conversely, the more frequently a cipher key is reused, the easier it is to break. Reuse of a cipher key allows the cryptanalyst to look for patterns or characteristics which might yield clues concerning the system. Thus, *a good cipher key does not repeat.*

This is a real problem for ciphers which run continuously because they quickly exhaust the key stream. One way of extending a key stream

XRFGP MDAPC VIQXM PQWZM COIQX ZMWQI

indefinitely is to feed the cipher text back into the key generator to extend the key. The previously ciphered text is added to the key stream to generate a new key which is then added to the new plain text. Thus, the plain text is a function of - (1) *the old key stream*, (2) *the old plain text*, and (3) *the new key stream*. Since transmission of a repeating message is unnecessary, it is unlikely that the plain text will repeat. Hence, *it is possible to generate a key stream of indefinite length.*

Another way of assuring that a key is never reused is to limit the length of messages. When a key is exhausted, another session key is used to generate a new key stream.

One way in which some ciphers make use of the "one time principle" is by using some variation of a master key for each message. Each variation of the master key is called a "session key."

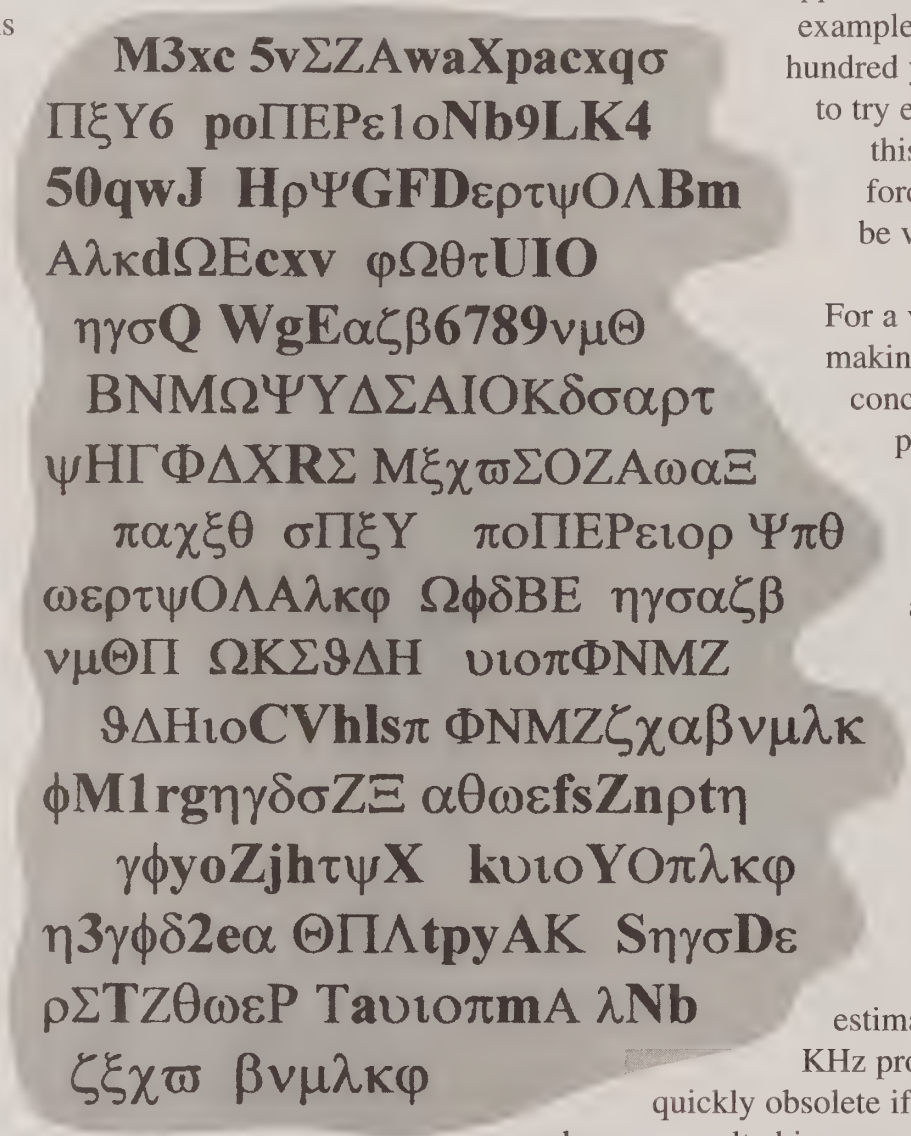
The cipher system should be designed so that it does not propagate errors if one piece of data is misread.

The principal difficulty in using old cipher text to extend a key stream is that it creates a cipher system which *propagates errors*. If the cipher text is received incorrectly, an error will enter the decryption key making it impossible to decipher the rest of the message.

Not all ciphers propagate errors in this fashion. However, if the cipher text is not used to extend the key, it is more difficult to generate a key stream which never repeats itself.

The cipher system should have a sufficient number of daily keys to preclude testing every possible key using special purpose computers operated in parallel at a speed much higher than the fastest available computer.

If a cipher algorithm is known, one method of breaking the cipher is to program a computer to try all possible key combinations. To preclude this from happening, a cipher key must have *a sufficiently large number of possible key combinations to make this approach impractical.* For example, if it would take a hundred years for a computer to try every possible key, this kind of "brute force" attack would not be very practical.



For a variety of reasons, making judgments concerning how many possible keys is enough can be a tricky business. Technology advances quickly. For example, suppose it would take a computer running a hundred years to check all possible keys for a particular cipher. A hundred year estimate based upon a 50 KHz processor would be quickly obsolete if technological advances resulted in processors which operated at 10 MHz, 100 MHz, or 400 MHz.

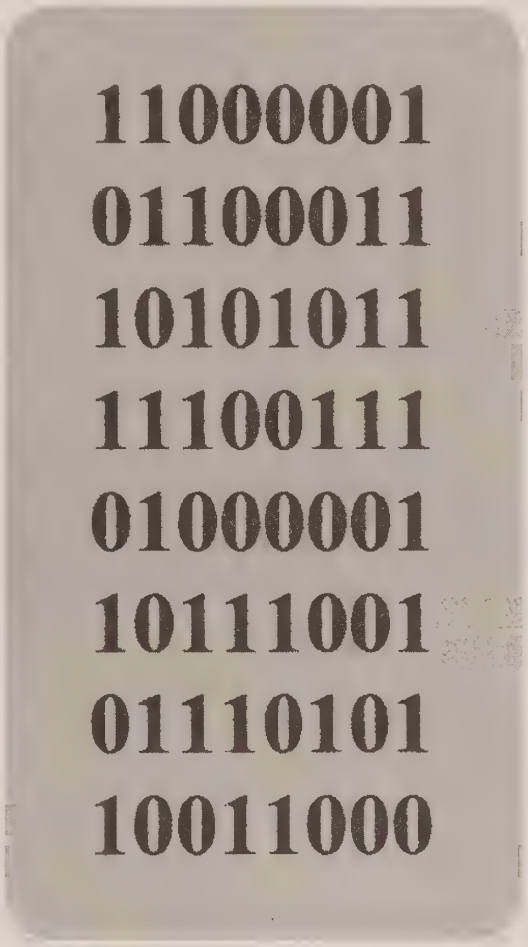
With a 10 MHz processor, it would take a maximum of one-half year to test all possibilities. With a 100 MHz processor breaking the same cipher would take a maximum of around 18 days. With a 400 MHz processor it would take a maximum of 4.563-days. Now, if *a special purpose computer* was designed to do the analysis at 400 MHz this estimate might be easily cut in half. If *ten special purposes*

computers were operated in parallel, it would take a maximum of 5.48-hours to break the cipher. However, it might in fact take less time. On average, the computers might have to test only half of the possible keys before hitting the "jack-pot." Hence, such a system would probably break the cipher in 2.74-hours.

This is essentially the method which the British used to break the famous *Enigma Cipher.* Thus, when Rommel's forces launched a "surprise" attack on American forces in North Africa, General Patton knew they were coming from *communications intelligence.* When the British fought the Battle of Britain they didn't have to count enemy losses. They simply read the German reports from decrypted German messages.

Poor cipher systems were a key factor in World War II. In fact, it is arguable that, despite being better prepared at the beginning of the war, Axis powers may have lost the World War II *because they relied upon poor cipher systems. A similar reliance upon cipher systems can be just as costly to a pay television enterprise.*

Because new technology can increase the speed of computer processors by a factor of a hundred or even a thousand, misjudgements are possible.



If an analyst discovers certain *flaws* in a target cipher *it might not be necessary to test all possible keys.* In that case it might only be necessary to test 10-percent of the possible keys. Hence, using ten 400 MHz special purpose computers operated in parallel, the cipher in the previous example might be broken in only 16.4-minutes.

Thus, a cipher which seems superficially secure because it has a large number of keys may in fact be easily broken because of flaws in the cipher and technological advances in processor speeds.

The cipher system should be designed so that the key or key stream itself is never "exposed" when there is no program input.

Ciphers which run continuously need to be designed so that the encryption key itself is never exposed. Because many digital keys bond the cipher key to the plain text, the "cipher text" will be identical to the cipher key when there is no plain text input unless precautions are taken to preclude this from happening. One way to prevent this from happening is to mix a *pseudo plain text stream* with the real plain text before the real plain text is bonded to the key.

Master keys should be totally random.

If key selection follows any system or pattern it is theoretically possible to predict the key. Random master keys are necessary to make the choice of keys *totally unpredictable.*

*Master keys should be changed daily.**

The reuse of a key increases the probability that analysis of the cipher text will reveal a pattern which could make the key easier to deduce.

*Master keys should never be sent over a communications link even if the link itself is enciphered.**

Master keys should never be transmitted over a communications link. The reason is obvious. If master keys are transmitted over a communications link, the new key cannot be any more secure than the old key. If the old key is compromised, someone intercepting the communication will get the new key.

*Master keys should be sent via mail or courier.**

The most secure means of transmitting master keys is by courier. For pay television purposes, the mail can be regarded as a secure means of

communications. Unfortunately, the mail is slow, costly, and cumbersome.

Each message should use a unique and random "session key" which is not reused again.

It has been said that a key should never be reused. Thomas Jefferson was one of the first to recognize that a "one time" code is almost impossible to break. In order to preclude reuse, some cipher systems use a special *session key* for *each message or message block*. A session key is usually some variation of a key stream based upon some particular master key. For example, a session key may be generated by adding some number to the master key for each message or message block. Thus no two messages or message blocks have exactly the same cipher text even if the same message is retransmitted.

Usually a session key is encrypted *using the master key* and then transmitted to the other station at the *beginning of each message*. Since no two session key are the same, the cipher text of every encrypted session key will be different. The receiving station then deciphers the session key using the master key and adds the session key to the master key for deciphering the message. One flaw which helped the British break *Enigma* was the fact that *Enigma never* enciphered a letter as itself. This flaw helped the British deduce *Enigma's* session key.

MDA PC VIQ POQ
XMPQWZM UR
V FDXSW P QE
C O IQX MMCX
W Q I MC MLKS
FDA ERPX MXZ

Each communications link in a network should use a unique and random "session key" which is not duplicated in any other link.

A *unique session key* for different communications links assures that compromise of one key will not compromise the entire network. Frequently session keys are generated by simply using a *random number generator*. Thus, even the operator does not know in advance what session key she or he will be using. For practical purposes, when session keys are generated in this way, each link in a network will use a different key.

*Keys must be kept secret.**

Military and diplomatic cipher systems *assume the integrity of the people operating the communications network.* It is for this reason that *communications security* is the single most sensitive field in which personnel can work. If a spy compromises a cipher key, the entire cipher system is worthless no matter how well designed it may be. The implications for the pay television industry should be obvious.

Cable and satellite programmers cannot assume the integrity of all subscribers. Any subscriber could be a "hacker" or a distributor of pirate equipment. For this reason, cipher systems are inappropriate for guaranteeing total program security.

*Plain text must be kept secret.**

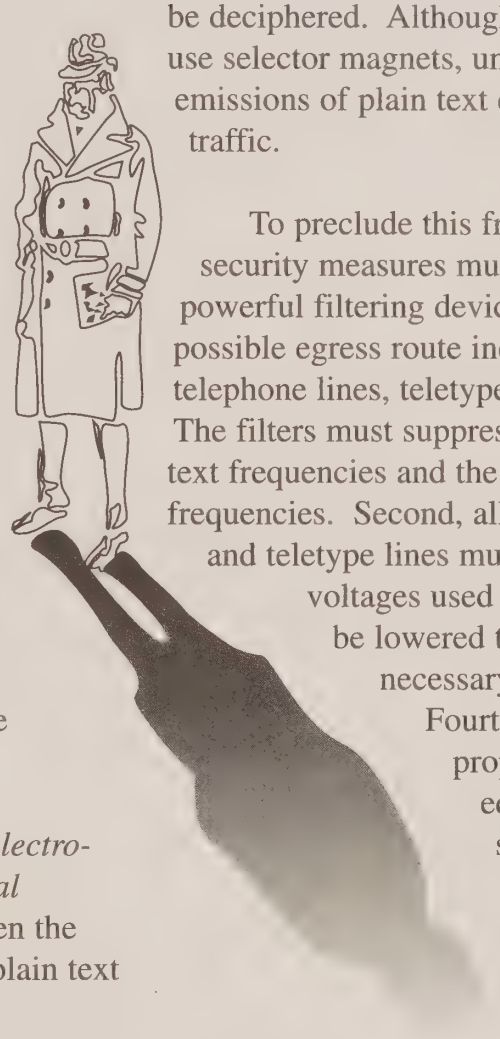
The security of a cipher system depends as much upon the security of the plain text as it does upon the security of the cipher key. If either is compromised, the other can be deduced. Since all program subscribers have access to both the program cipher text and the program plain text, all subscribers have everything necessary to deduce the key. Hence, it is impossible to keep the cipher key secret from the recipient of the program. Hence, all subscribers have access to the cipher key. The implications for the security of DBS satellite broadcasting should be obvious.

Because any subscriber could be a "hacker" or "pirate distributor," any pirate distributor can gain access to sufficient information to deduce any cipher key if the hacker or distributor has the required equipment and expertise.

Ultimately pay television security is not to be found in the field of cryptography. The success of a business depends upon keeping costs low and sales high. *Excessive reliance upon poor cipher systems can produce exactly the opposite results for a pay television operator.* When millions of dollars are

invested in a complex but flawed cipher system, costs are high as revenue goes down due to piracy. As rates are pushed up, a greater share of the final burden falls upon honest subscribers who become more inclined to disconnect service. Likewise, the incentive to pirate service is increased. More disconnects lower revenue. The ultimate result could be bankruptcy.

These facts also have serious implications for the security of commercial C-Band up-links and down-links. One way of solving the commercial security distribution problem would be to digitally multiplex programs together on a satellite transponder along with some pseudo program. By including a pseudo program which is not available to the public and by maintaining the security of exactly which programs are on specific transponders, the exact multiplexed plain text could be effectively concealed. By keeping the exact composite plain text secure, the key would be much more difficult to deduce. While this will work for *commercial links* to CATV systems, it will not work with DBS distribution systems for reasons which have already been explained. Efforts to "secure" programs on video tape cryptographically are equally futile.



TEMPEST. The unintended *transfer of electro-magnetically propagated emissions and signal transmissions* can completely circumvent even the best encryption systems. This occurs when plain text artifacts unintentionally leak out of a secure communications installation.

During the "cold war" professional "spooks" and "spies" learned that it was possible to set up an extremely sensitive receiver near certain secure installations and monitor "plain text" emissions from the installation's teletypes. Older teletypes used to have selector magnets. A teletype's contacts create sparks when they open and close. These sparks create unique electro-magnetic emissions which could be transferred outside the installation through a variety of egress routes. These routes could include the installation's power lines, the installation's telephone lines, the installation's ground system, or through the walls of the facility.

When plain text emissions leak out of a secure facility the result can be a *catastrophic security compromise*. Monitors sitting outside the facility need only obtain enough plain text to determine the settings of the key generators used for encrypting secure traffic. Once these settings are determined, all of the secure traffic encrypted using those settings can be deciphered. Although modern equipment does not use selector magnets, unintended radio frequency emissions of plain text can still compromise secure traffic.

To preclude this from happening a variety of security measures must be implemented. First, powerful filtering devices must be used on all possible egress route including power lines, telephone lines, teletype lines, and so forth. The filters must suppress both the fundamental plain text frequencies and the harmonics of those frequencies. Second, all power lines, telephone lines, and teletype lines must be shielded. Third, the voltages used in "plain text" circuits should be lowered to the minimum levels necessary to operate the equipment. Fourth, all equipment must be properly grounded. Fifth, all equipment must be properly shielded. Air vents should be protected with metallic screens to prevent emissions through vent openings. Finally, equipment should never be operated with open chassis covers.

The hazards posed by TEMPEST with respect to the security of all cryptographic systems demonstrates the futility of attempting to rely upon cryptography to secure widely disseminated programming. Whenever the plain text of a secure communication is widely available it is relatively easy to use that plain text with the public cipher text to deduce the key used to encrypt the traffic.

Works Consulted

Henry Becker and Fred Piper, ***Cipher Systems: The Protection of Communications.*** New York: John Wiley and Sons, 1982.

Bruce Bosworth, ***Codes, Ciphers, and Computers: An Introduction to Information Security.*** Hasbrouck Heights, New Jersey: Hayden Book Company, Inc., 1982.

Helen Fouche Gaines, ***Cryptanalysis: A Study of Ciphers and Their Solution.*** New York, N.Y.: Dover Publications, 1939.

Norma Gleason, ***Cryptograms and Spygrams.*** New York, N.Y.: Dover Publications, 1981.

F.H. Hinsley and Alan Stipp, eds., ***Code Breakers:The Inside Story of Bletchley Park.*** Oxford, England: Oxford University Press, 1993.

David Kahn, ***The Codebreakers: The Story of Secret Writing.*** New York, N.Y.: Macmillan Company, 1967.

Henry Lysing, ***Secret Writing: An Introduction to Cryptograms, Codes, and Ciphers.*** New York, N.Y.: Dover Publications, 1974.

Norman Polmar and Thomas B. Allen, ***Spybook: The Encyclopedia of Espionage.*** New York: Random House, 1977.

Lawrence Dwight Smith, ***Cryptography: the Science of Secret Writing.*** New York, N.Y.: Dover Publications, 1971.

---------- ***Understanding Computers: Computer Security.*** Alexandria, Virginia: Time-Life Books, 1986.

Peter Way, ***Codes and Ciphers.*** New York, N.Y.: Dover Publications, 1977.

Chapter 12
Special Filters & Filtering Networks

A number of special purpose filters and special filtering networks are made for a variety of applications. These include filters for solving interference problems and special pay television filtering networks. Pay television filters may also be used for solving a variety of interference problems which were previously solved using custom filters. Special purpose pay television networks are frequently used to reduce the costs associated with serving *multiple dwelling units* (MDUs).

Amplitude Equalizers

Although coaxial trunk amplifiers and main-station amplifiers contain *automatic slope controls* (ASCs) to equalize signal levels, it is still possible to have some line-tilt on long coaxial drop-lines. Line-tilt arising from feeder lines, drop-lines and drop-line filters may require equalization. A variety of *amplitude equalizers* are made for equalizing the coaxial drop-line tilt. Equalization slopes range between 1.25 and 8.75 dB (measured from the bottom of the band). Typical specifications are listed in Table 12.1. Circuitry is built into a standard cylindrical enclosure with male and female connectors at each end.

Ingress Interference

In general radio frequency interference may be classified as either - (1) *differential mode interference*, or (2) *common mode interference. Differential mode interference* typically involves either *in-band interference* or *out-of-band* interference mixed with the desired signals in the radio frequency spectrum. In a cable system this type of interference enters the system on the center conductor of the coaxial cable. Differential mode interference can also enter a system through openings in the equipment case. *Common mode interference* differs from differential mode interference in that it enters equipment through the ground system. Typical routes include *ground leads* or the *coaxial cable shield.*

Ingress Suppression Filters

The spectrum below the VHF Low Band between 5 MHz and 42 MHz is frequently used as a *high speed return path.* Typical applications include *PPV*, *IPPV*, and *Internet* applications. Unfortunately, the spectrum below 42 MHz has a number of difficulties. A variety of interference sources emit signals below 42 MHz. These sources include Ham Radios, Citizens Band Radio Transmitters, and a variety of home appliances. Ingress suppression filters prevent noise and interference from entering the CATV distribution network. Figure 12.2 illustrates the high-pass response of a typical ingress suppression filter. The response shown in Figure 12.3 contains a *return*

DROP-LINE AMPLITUDE EQUALIZERS

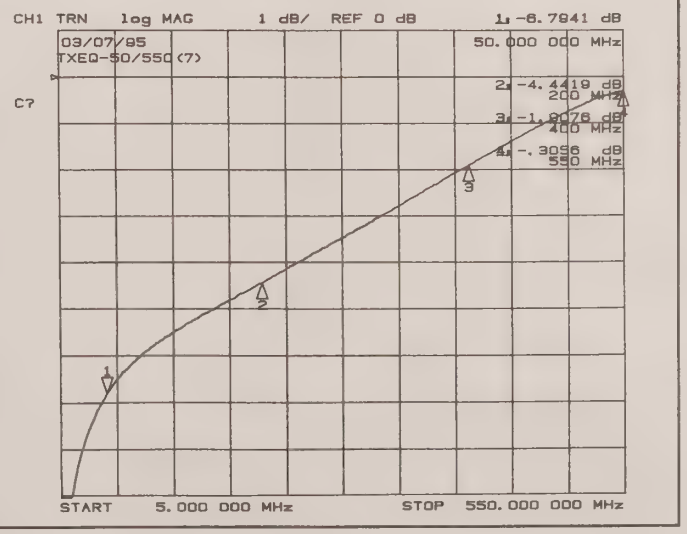
Typical Specifications

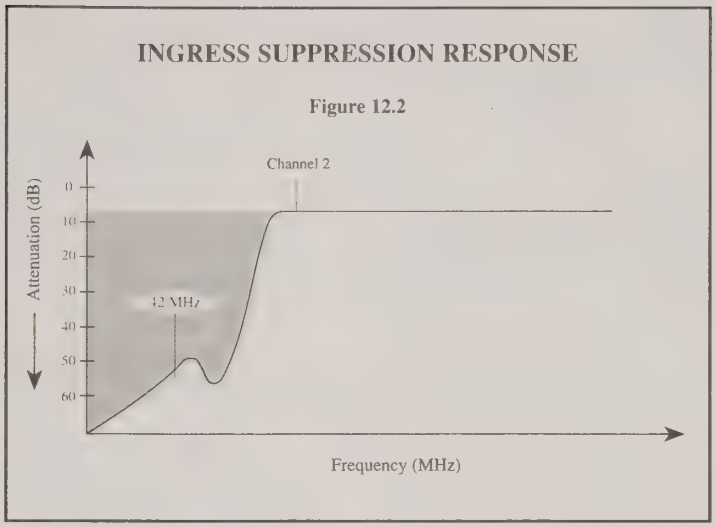
Table 12.1

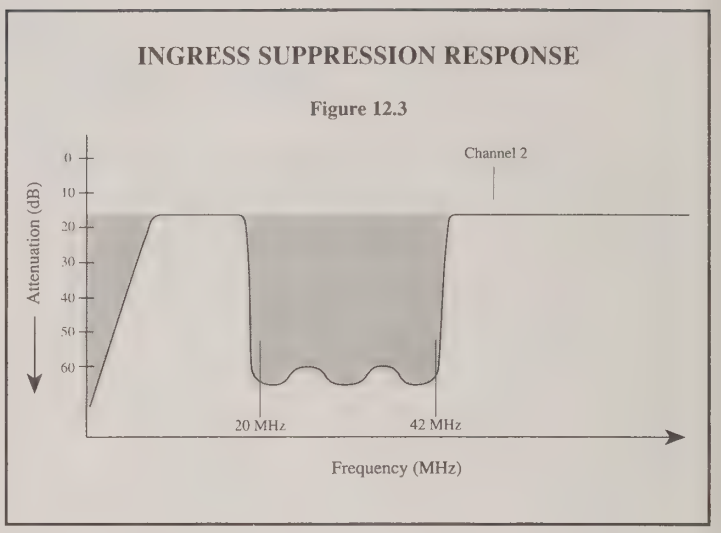
Bandwidth:	**300, 400, 450, 500, or 550 MHz**
Insertion Loss:	**1.0 dB (maximum)**
Return Loss:	**16 dB**
Equalization Slope:	**1.25 to 8.75 dB**
Temperature Range:	**- 40 to + 140 degrees Fahrenheit**
Temperature Drift:	**< +/- 0.5 dB over range**
Impedance:	**75 ohms**
Connectors:	**Type F (male & female)**
Diameter:	**7/8th inch (tubular)**
Length:	**2.5 inches**
Weight:	**2.9 ounces**

A DROP-LINE EQUALIZER

Figure 12.1







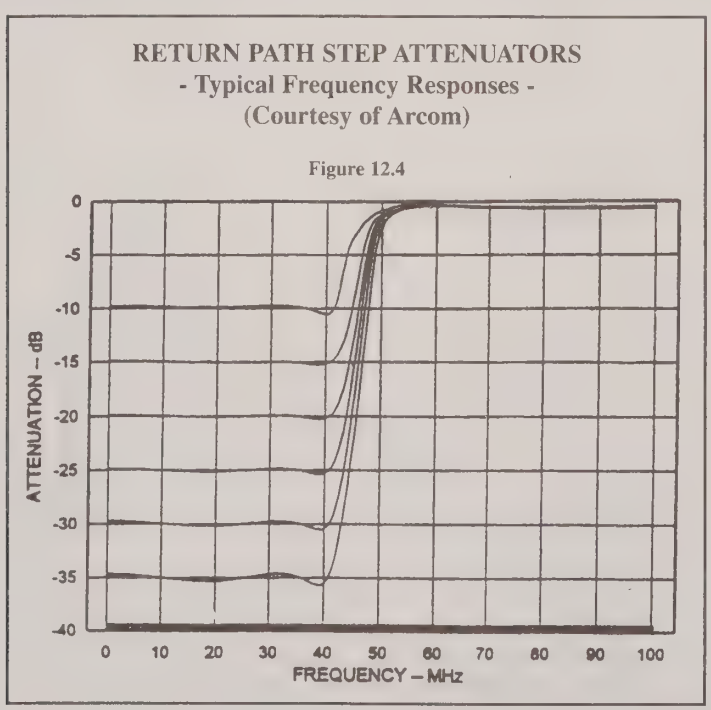
path window for use with two-way set-top converters or computer modems.

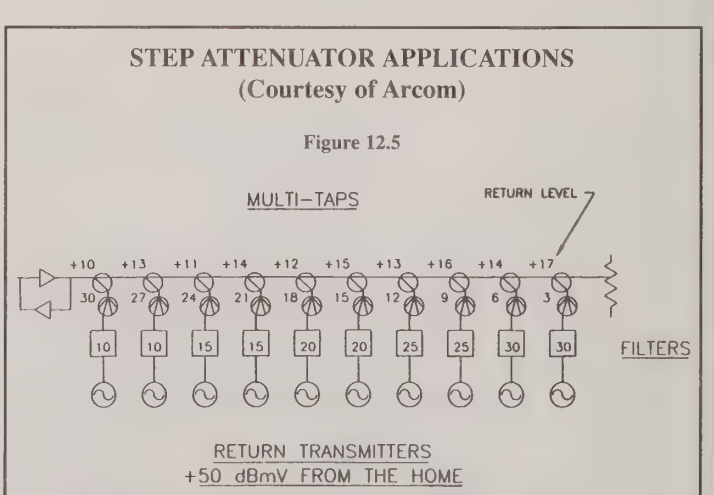
Return Spectrum Step Attenuators. Problems involving the use of the VHF sub-band, below 42 MHz, as a return path are not limited to merely preventing subscriber generated interference from entering the distribution network. For subscribers who do not need a return path it is possible to prevent interference from entering the network by placing a low pass filter on the drop-line. However, *whenever a substantial number of subscribers need to use the return path* the problem of reducing subscriber generated interference becomes more complex.

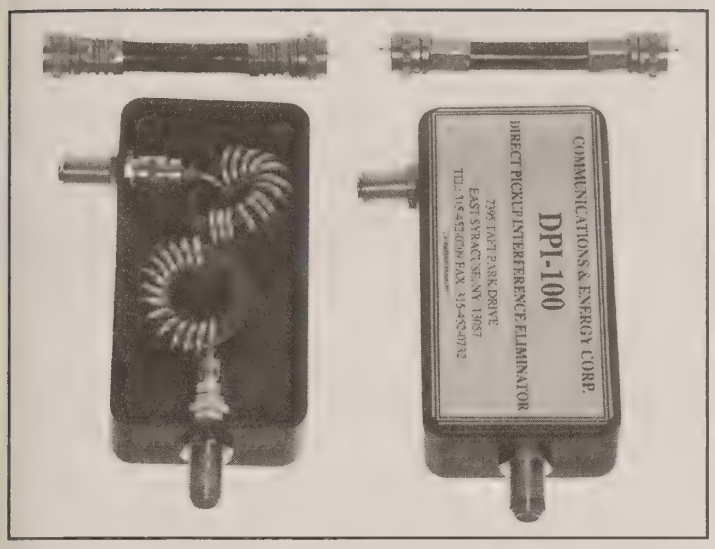
Because cable distribution networks have a tree like design, interference generated at each tap in the return path spectrum is additive. Thus, as more subscribers use the return path spectrum, the level of interference in that spectrum will increase. This problem is further complicated by two additional considerations. First, because of line-tilt, the return path response will vary as one more moves further from the headend. Second, return path signals from taps located further from the headend require more amplification than those located near the headend. Consequently, interference generated at taps located furthest from the headend creates more problems than interference generated at taps near the headend.

One way of solving this problem is to equalize return path signal levels. This can be done by placing a specific value attenuator in the drop-line of each tap in the system. The value of the attenuator chosen for any specific tap depends upon the distance of the tap from the headend. Thus, the attenuator values increase as one moves further and further from the headend.

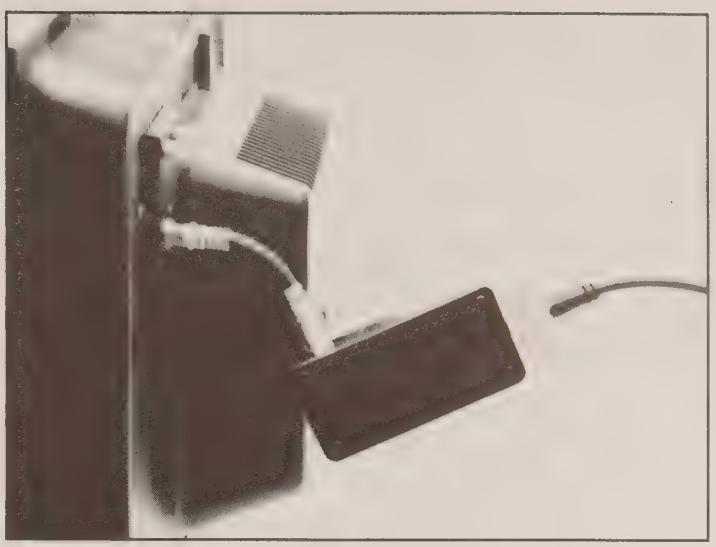
Direct Pick-Up Interference. With the introduction of cable compatible television receivers an increasing number of subscribers are becoming victims of DPI. The problem also affects *Master Antenna Television* (MATV) systems. Virtually all




STEP ATTENUATOR APPLICATIONS
(Courtesy of Arcom)
Figure 12.5
MULTI-TAPS
RETURN LEVEL
+10 +13 +11 +14 +12 +15 +13 +16 +14 +17
30 27 24 21 18 15 12 9 6 3
10 10 15 15 20 20 25 25 30 30
FILTERS
RETURN TRANSMITTERS
+50 dBmV FROM THE HOME



A typical coaxial shield filter (Photo by C&E Corp.)



Coaxial shield filters are installed on the input of a television set or VCR (Photo by C&E Corp.)

elevision receivers currently on the market suffer rom DPI when strong ambient RF fields are resent. Computer studies undertaken by *Stern Telecommunications Inc.* in 1992 indicate that erhaps 48-percent of television house holds ould be subject to DPI from VHF/UHF television tations operating below 550 MHz.[1] Given the large umber of non-television transmitters operating etween 18 MHz and 550 MHz, the total potential for DPI is probably above 48-percent. Further, a growing umber of LPTV stations and transmitters in other adio services continue to be licensed every year. Fiber optic systems will not solve such problems as long as coaxial drop lines are used.

Direct pick-up interference (DPI/DPU) is a form of common mode ingress interference which enters a subscriber's television receiver *on the coaxial drop line shield.* DPI enters a television tuner on the shield of a coaxial input cable. DPI symptoms may be broadly classified as either - (1) *coherent* interference, or (2) *non-coherent* interference.

Coherent interference is defined as any form of interference which results in the simultaneous display of two pictures at the same time. Typically an unwanted picture is superimposed faintly in the background of a stronger desired picture. Examples of coherent interference include - (1) same picture ghosting (like multiple reflections on an antenna

[1]J.L. Stern, Direct Pick-Up Interference, in ***Communications Technology.*** July 1993, p. 51.

INGRESS SUPPRESSION FILTER

Typical Specifications

Table 12.2

Passband:	**5 MHz to 13 MHz**
	50 MHz to 1 GHz
Insertion Loss:	**1.5 dB (maximum)**
Stopband:	**16 MHz to 40 MHz**
Stopband Suppression:	**40 dB (minimum)**
Temperature Range:	**- 40 to + 140 degrees Fahrenheit**
Temperature Drift:	**< +/- 0.5 dB over range**
Impedance:	**75 ohms**
Connectors:	**Type F (male & female)**
Diameter:	**7/8th inch**
Length:	**2.25-inches**
Weight:	**2-ounces**

COAXIAL SHIELD FILTER SPECIFICATIONS

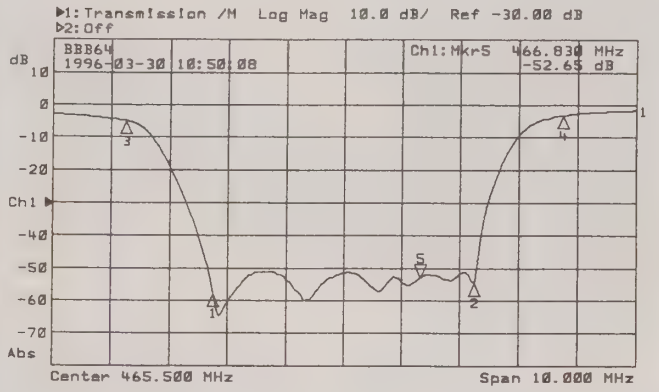
Typical Specifications

Table 12.3

Effective Beat Frequency Reduction:	**40 MHz to 225 MHz**
Operating Frequencies:	**0 to 550 MHz**
Insertion Loss:	**0.6 dB**
Return Loss:	**-18 dB**
RF Shielding:	**100 dB**
Impedance:	**75-ohms**
Connectors:	**Type F (female)**
Net Weight:	**3.5 oz.**
Size:	**4 x 2 x 7/8-inches**

FREQUENCY RESPONSE OF CHANNEL DELETION FILTER

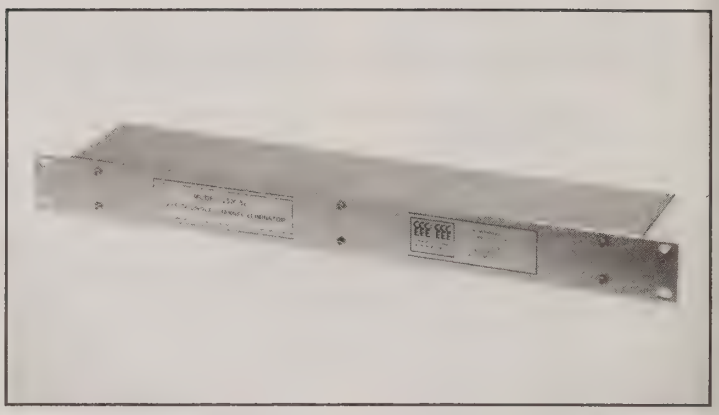
Figure 12.6



system), and (2) co-channel interference (when a different picture is superimposed in the background).

Non-coherent interference is defined as any unintelligible interference pattern in a television picture. Some examples of non-coherent patterns include horizontal, vertical, or diagonal lines. Other patterns include *rolling lines*, a *rolling picture*, *barber pole lines*, *bars*, *tearing*, *wavy lines*, *herringbone*, *venetian blinds*, "*sparklies*", *snow* in the picture, *color distortion*, an *audio buzz*, *pale colors*, or a *windshield wiper* effect.

Solution. Because ingress interference can enter a receiver though a variety of different routes - including the power supply, tuning holes in the tuner chassis, and on the shield of the coaxial drop line - each case must be carefully diagnosed.[2] All ingress



Typical channel deletion (Photo by C&E Corp.)

routes must be closed. A coaxial shield filter may be used to stop ingress on the drop-line shield. Table 12.3 gives typical filter specifications.

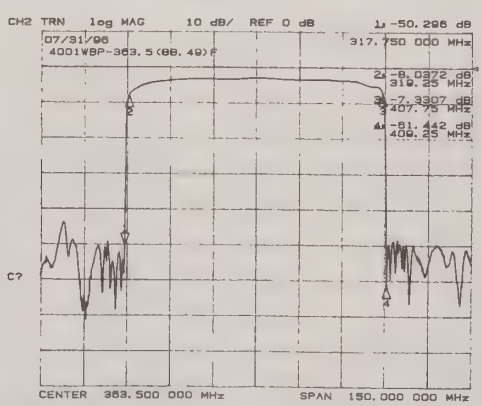
Special Networks

Highly selective *bandpass filters* (BPFs) and channel deletion filters (BSFs) may be used to build a variety of special purpose filtering networks for use in *multiple dwelling units* (MDUs). Large apartment buildings, hotels, and motels represent typical examples. Opportunities sometimes arise where a cable operator may want to provide specialized services to customers without having to put a set-top converter in every unit. For example, a two-hundred room hotel might want to provide a premium channel, like HBO, to its guests as part of the room fee. In

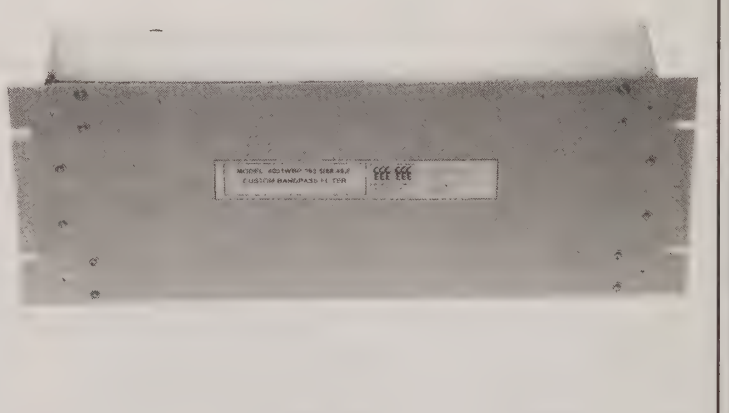
[2]Cf. Glyn Bostick, Ronald E. Mohar, and Vince Cupples, "Suppressing Direct Pick-Up Interference," Parts I, II, and II in ***Communications Technology*** for diagnostic procedures.

HIGH SELECTIVITY BANDPASS FILTER

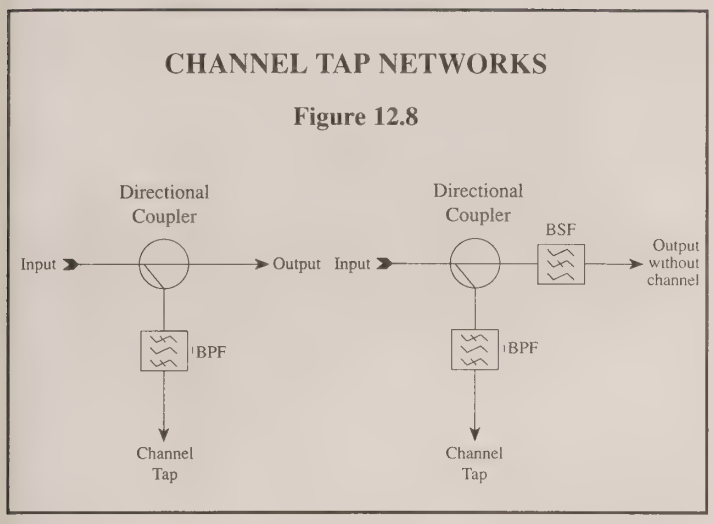
Figure 12.7



Frequency response of a highly selective band-pass filter. The skits fall 50 dB in 1.5 MHz.



A highly selective bandpass filter (Photo by C&E Corp.)



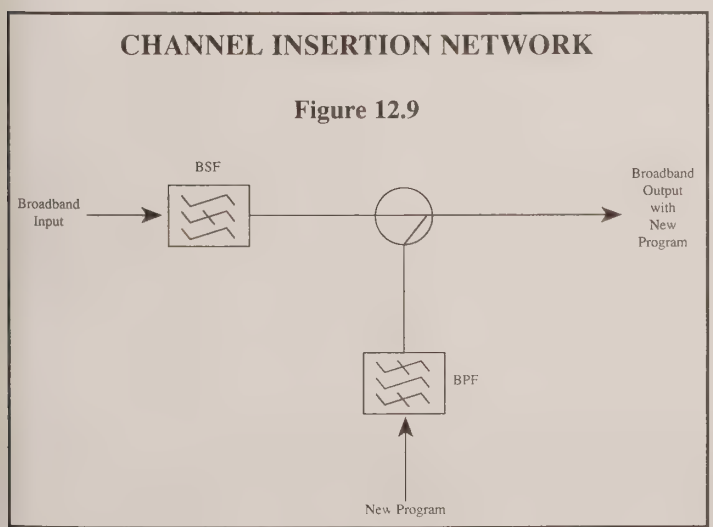
that case the cable operator might contract to provide the service based upon actual occupancy rates.

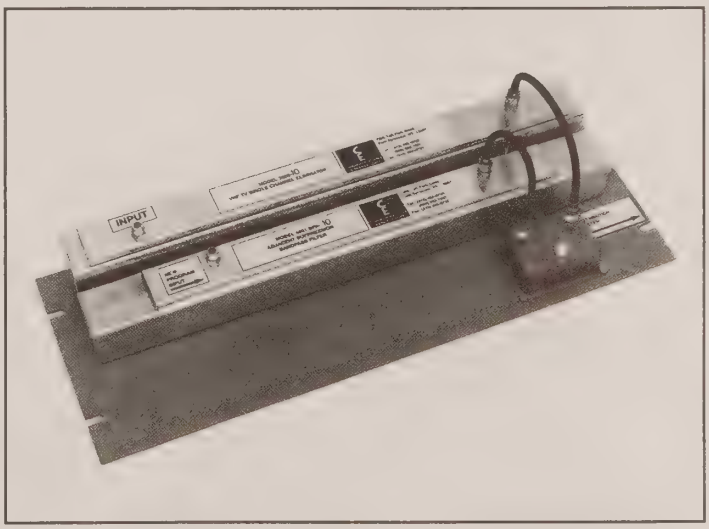
Channel Deletion Filters. Unlike typical pay television traps, *channel deletion filters* are designed to suppress everything within a 6 MHz channel by 50 dB or 60 dB so that a new program can be inserted in place of the old program. Channel deletion filters must have steep skirts and narrow guardbands in order to minimize attenuation on adjacent channels. Passband ripple should be minimized in order to minimize distortion. Channel deletion filters can be built to be either DC passing or DC blocking.

Bandpass Filters. Bandpass filters are used in specialized filtering networks to filter inputs and outputs. When a program is reinserted into a channel spectrum between two other programs, noise and interference on the adjacent channels must be minimized. Most channel modulators have bandpass filters on their outputs. However, as a modulator ages, it sometimes outputs spurious signals on adjacent channels. It is particularly important to use a powerful bandpass filter on modulator outputs when inexpensive modulators are used because the output bandpass filters may not be very good.

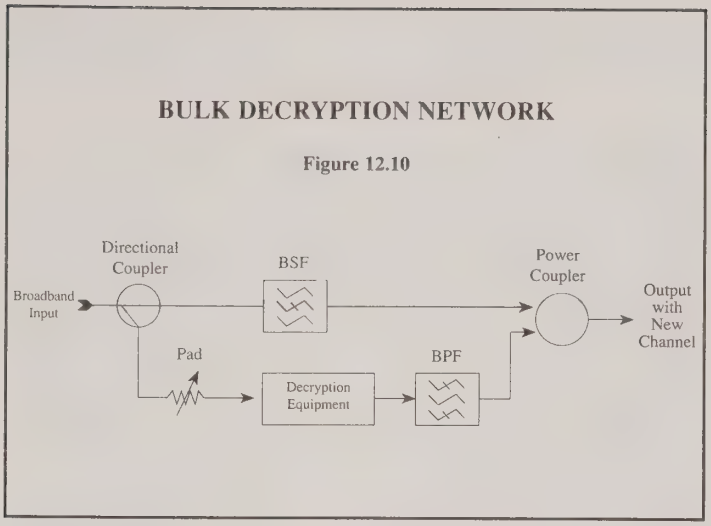
Channel Taps. A directional coupler and a bandpass filter may be used to build a channel tap as illustrated in Figure 12.8. The first unit taps off a channel while passing the original spectrum to other subscribers unchanged. A channel deletion filter is used in the second tap to remove the channel so that an empty channel is passed to other subscribers. If the bandpass filter is highly selective, the adjacent channel spectrum will be "clean." Hence, the adjacent spectrum may be used for insertion of other programs.

Channel Patch-In Networks. Channel deletion and insertion networks may be used for a variety of applications. Figure 12.9 shows a typical network. For example, a channel deletion and insertion network may be used to remove a cable channel from a broadband spectrum in an apartment building so that a picture from a lobby *security camera* may be inserted into the distribution network. Residents may then tune to a specific channel to see who is at the front door before "ringing them in" with a remote door latch. Such a network could also be used to insert *locally originated programs* or to take a program from one channel and put it on another channel. Other applications include inserting a program from a satellite dish, a local VHF antenna, a local UHF antenna, or a wireless (MMDS) antenna.



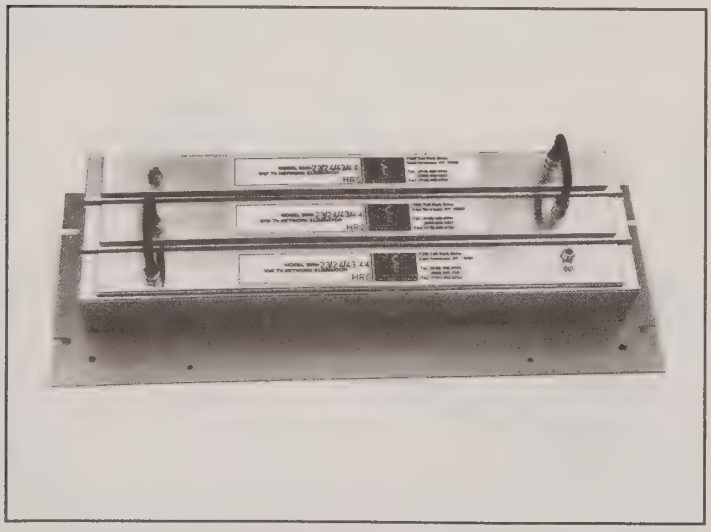


A channel insertion network (Photo by C&E Corp.)

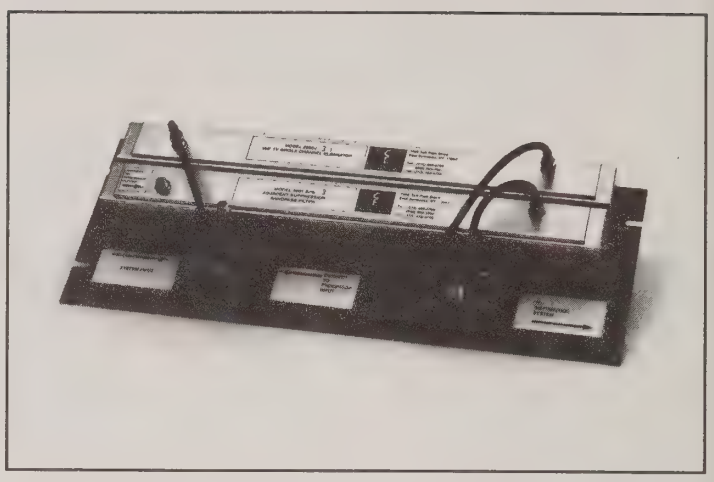


Batch Decryption Networks. Batch decryption networks are used where an operator wants to supply an MDU with one or more premium channels without equipping every unit with a set-top converter. In a large hotel or apartment building such a network could save an operator thousands of dollars and eliminate a considerable amount of maintenance. Figure 12.10 illustrates a typical network. It is made using a channel tap and a channel deletion and insertion network.

The channel tap picks an enciphered channel off the network and feeds the program to a set-top converter or deciphering equipment. A channel deletion filter removes the program from the broadband spectrum and makes a space to reinsert the channel. The deciphered channel is then re-inserted into the empty channel through a bandpass filter. A 3 dB attenuation pad is used to equalize channel levels. The power coupler is used to combine the new channel with the other channels. Similar



A multi-channel deletion filter (Photo by C&E Corp.)



A bulk decryption network (Photo by C&E Corp.)

networks may be designed for multiple channels.

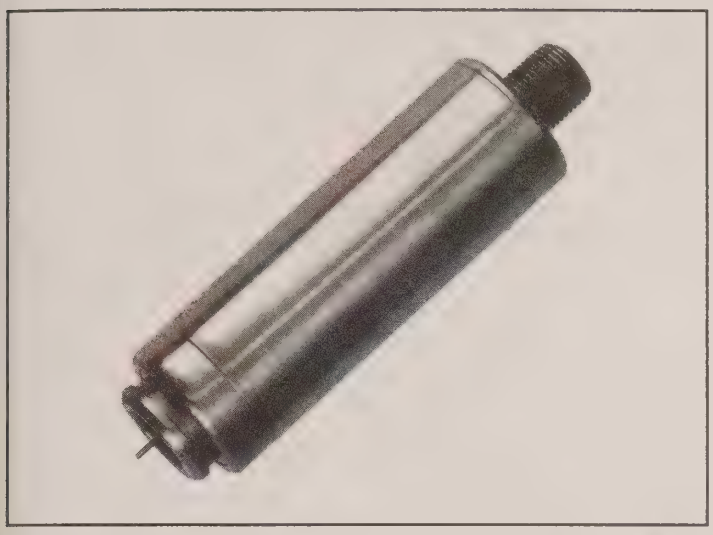
Other Networks. The network shown in Figure 12.10 may also be used as a bulk encryption network by substituting an encryption device for the decryption device. For example, a cable operator could encipher a clear channel using a positive security system for use inside an MDU. A trap would then be placed on each subscriber's distribution line. Since the number of subscribers in the MDU is limited, it is unlikely that a pirate would bother to try to produce pirate traps for such a limited market.

The network shown in Figure 12.10 is not limited to use with decryption and encryption devices. By substituting a demodulator and a modulator, a channel converter, or a processor for the decryption device, the network may be used for a wide variety of other purposes. For example, using an amplifier in the circuit, it is possible to boost the level of a weak channel back up to the level of adjacent channels.

Solving Interference Problems

In many situations it is possible to use pay television filters to solve a variety of interference problems which used to be solved using custom filters. Because of their unique weatherproof enclosure, pay television filters are well suited for outside applications in antenna down-leads. It is also possible to retune existing pay television filters at the factory in order to customize them for special applications.

Highpass & Lowpass Filters. Highpass and low-pass filters are among the most useful devices for



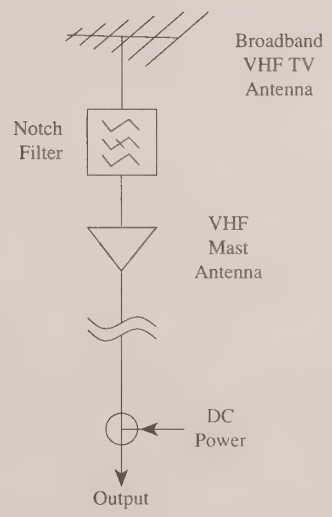
solving certain kinds of interference problems. For example, Citizens Band Radio frequencies and a number of Ham Radio bands are located below the VHF Low Band. These frequencies can often interfere with television receivers if the transmitter is located near enough to the television receiver.

The usual remedy is to place a lowpass filter with sufficient power handling capacity on the transmitter's output. However, if that approach is not sufficient to completely remedy the problem, remedies at the receiver are also possible. A highpass pay television filter tuned to cut-off just below VHF Channel 2 will block reception of all below band frequencies.

One of the advantages of using a highpass filter is that one does not have to know the specific interference frequency. All one has to know is that below band interference is the source of the problem.

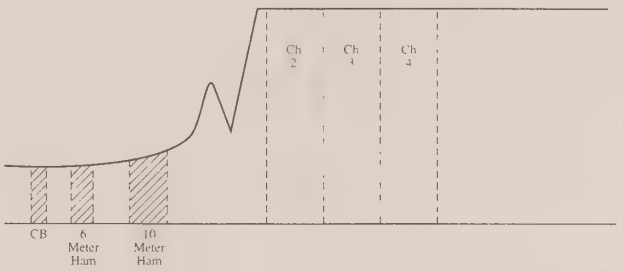
INTERFERENCE NOTCH FILTER

Figure 12.12



HIGHPASS FILTER

Figure 12.11



Hence, highpass filters and lowpass filters are useful when the interference frequencies change from time to time.

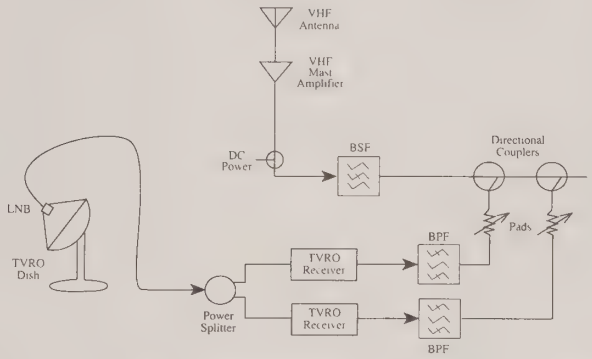
Notch Filters. Notch filters are useful remedies when a particular fixed frequency is causing a problem. Suppose a situation in which the visual carrier from a nearby television transmitter is over-loading the preamplifier for on a antenna used for receiving an out-of-town station. If the transmitter is operating on VHF Channel 2 and the reception antenna is receiving on VHF Channel 4, it would be possible to place a Channel 2 negative trap in the down-lead to suppress the problem frequency. Similar applications exist in the FM band. Figure 12.12 illustrates a typical application.

Suppose an FM transmitter operating near a residential neighborhood which is over-loading all of the FM receivers the area. This can be a real problem because the automatic frequency controls (AFCs) on FM receivers will lock onto the strongest carrier and de-tune the receiver from the desired frequency. One possible remedy might be to return the notch on a Channel 95, 96, or 97 negative trap to the problem frequency in order to suppress the problem carrier. Although one would probably lose the adjacent FM channels, adjacent channel FM stations are never licensed in the same area anyway.

Sometimes transmitters operating near a receiver can cause intermodulation in a reception system even though there is a considerable separation between the interfering frequency and the desired reception frequency. If signal levels are strong enough, intermodulation can create beat frequencies all across the reception band effectively "jamming" the whole

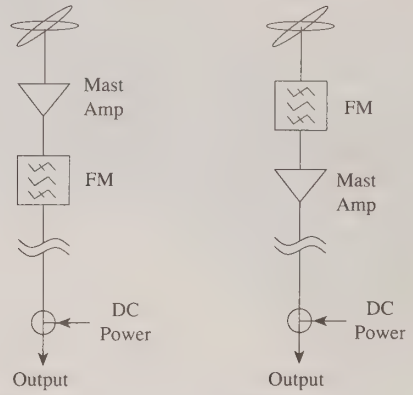
LOW COST CHANNEL INSERTION NETWORK

Figure 12.13



FM BANDPASS FILTER

Figure 12.14



band. The solution is simply to tune a notch to the problem frequency and place it in the antenna down-lead.

Tier Filters. Mid-band tier filters are very common because numerous cable operators use the mid-band as a second tier. In some cases, a mid-band tier filter may be used to make an *inexpensive channel insertion* network for an MATV system as illustrated in Figure 12.13. Such a system might be used in a small a home or a small motel.

Suppose that the customer wants to connect a number of specific TVRO channels into a broadband VHF reception and distribution system. Because a broadband VHF antenna usually receives signals in the mid-band, it is not possible to simply re-modulate signals from a TVRO receiver and insert them into the network on Channels 14 to 22. One low cost solution might be to place a mid-band tier filter in the down-lead from the broadband antenna. The mid-band stop filter will suppress all signals from the antenna in mid-band and make nine "parking spaces" for new channels. A bandpass filter should be used at the output of each TVRO modulator to assure that spurious modulator emissions do not interfere with adjacent channels.

Bandpass Filters. Pay television bandpass filters are sometimes used to provide individual channels or groups of channels to subscribers who do not want to subscribe to an entire tier. As illustrated in the previous example, such bandpass filters can be useful on low cost modulators for suppressing spurious modulator emissions. They may also be used for protecting specific channels from dedicated antennas which are cut-to-channel.

FM bandpass filters can be useful in situations where one needs to receive the entire FM band and suppress interference in the VHF High Band and the VHF Low Band. The filter is simply placed in the antenna down-lead. This approach has the advantage of suppressing interference on unanticipated interference frequencies. If a mast amplifier is used and the interference is not over-loading the mast amplifier, the bandpass filter should be placed in the line after the amplifier. This will minimize insertion loss between the antenna and the amplifier maximizing carrier-to-noise ratios. However, if amplifier over-load is likely to be a problem, then the bandpass filter should be connected in front of the mast amplifier in order to protect it.

Works Consulted

Glyn Bostick, John Fannetti, & William Johnson, ***ASTI: the Avoidance/Suppression Approach to Eliminating Terrestrial Interference at TVRO Earth Station.*** East Syracuse, New York: Microfilco Press, 1982.

Glyn Bostick, Ronald E. Mohar, and Vince Cupples, "Suppressing Direct Pick-Up Interference," Part I in ***Communications Technology.*** December 1995, pp. 54, 56, 58.

Glyn Bostick, Ronald E. Mohar, and Vince Cupples, "Suppressing Direct Pick-Up Interference," Part II in ***Communications Technology.*** February 1996, p. 66, 68, 70.

Glyn Bostick, Ronald E. Mohar, and Vince Cupples, "Suppressing Direct Pick-Up Interference," Part III in ***Communications Technology.*** April 1996, pp. 56, 58.

Walter Ciciora, "the Direct Pick-Up Problem" in ***Communications Engineering & Design.*** June 1990.

Hugh W. Denny, ***Grounding for the Control of EMI.*** Gainesville, Virginia: Don White Consultants, Inc., 1983.

Eagle Comtronics, Inc. "How Ingress Suppression Traps Work" [Informational Monogram]. Clay, New York: Eagle Comtronics Inc., nd.

Federal Communications Commission, ***Interference Handbook.*** 1993 ed. Washington, D.C.: US Government Printing Office, 1993. Comtronics, Inc., nd., pp. 1-2.

General Instruments Corporation, ***CATV Reference Guide RD 16***. Brownsville, Texas: GI Communications, 1995.

Ed Hare and Robert Schetgen, eds., ***Radio Frequency Interference: How to Find It and How To Fix It.*** Newington, CT: American Radio Relay League, 1991.

Ron Hranac, "Combating Impulse Noise in Two-Way Systems" in ***Communications Technology.*** July 1996. pp. 16, 18, 20.

Ron Hranac, "Combating Impulse Noise with Common Mode Suppression" in ***Communications Technology.*** August 1996. pp. 16, 17, 18.

Charles L. Hutchinson, ed., ***The ARRL Handbook for the Radio Amateur.*** 62nd ed. Newington, CT: American Radio Relay League, 1985.

Charles L. Hutchinson and Michael B. Kaczynski, eds., ***Radio Frequency Interference: How Identify and Cure It.*** Newington, CT: American Radio Relay League, 1984.

Magnavox CATV Systems, Inc., ***Cable TV Reference Guide.*** Manlius, New York: North American Philips Corporation, 1991.

Michael Mardiguian, ***How to Control Electrical Noise.*** Gainesville, Virginia: Don White Consultants, Inc., 1983.

Ralph Morrison, ***Grounding and Shielding Techniques in Instrumentation.*** 2nd ed. New York: John Wiley & Sons, 1977.

Ralph R. Nelson, ***Interference Handbook.*** Wilton, CT: Radio Publication, Inc., 1981.

Joseph L. Stern, "Direct Pick-Up Interference in a World Without Converters" in ***Communications Technology.*** July 1993.

Donald R.J. White, ***Electromagnetic Shielding: Materials and Performance.*** 2nd ed. Gainesville, Virginia: Don White Consultants, Inc., 1980.

Steven M. Wollmerschauser and David M. Mundy, ***US Patent No. 5,091,707A.*** [filed August 30, 1990 & granted February 25, 1992]. Washington, DC: US Department of Commerce, Office of Patents & Trade Marks, 1992.

Appendix A
Reference Tables

COAXIAL CABLE INSERTION LOSS*

Per 100 Feet @ Frequency (MHz)

Table A.1

Frequency (MHz)	Loss (dB) RG-11	RG-6	RG-59
5	0.38	0.81	1.22
55	1.03	1.60	2.06
211	2.01	3.08	3.94
270	2.30	3.50	4.47
300	2.43	3.70	4.72
330	2.55	3.89	4.96
400	2.83	4.30	5.48
450	3.02	4.58	5.83
550	3.36	4.07	6.47
750	3.99	4.81	7.62
870	4.33	5.21	8.24
1000	4.67	5.62	8.87

*Exact values vary from one manufacturer to another.

CONVERSION BETWEEN dBmV and dBm

Table A.2

Conversion	Factor
dBm to dBmV	+ 49.75 dB
dBmV to dBm	- 49.75 dB

VHF TELEVISION CHANNELS

Table A.3

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
VHF-Sub	T-7	5.75-11.75	7.00	10.58	11.50
	T-8	11.75-17.75	13.00	16.58	17.50
	T-9	17.75-23.75	19.00	22.58	29.50
	T-10	23.75-29.75	25.00	28.58	29.50
	T-11	29.75-35.75	31.00	34.58	35.50
	T-12	35.75-41.27	37.00	40.58	41.50
	T-13	41.75-47.75	43.00	46.58	47.50
	TV-IF	41-47	45.75	42.17	41.25
VHF-Low	2	54-47	55.25	58.83	59.75
	3	60-66	61.25	64.83	65.75
	4	66-72	67.25	70.83	71.75
	5	76-82	77.25	80.83	81.75
	6	82-88	83.25	86.83	87.75
FM-Pseudo	95 FM-1*	88-94	89.25	92.83	93.75
	96 FM-2*	94-100	95.25	98.83	99.75
	97 FM-3*	100-106	101.25	104.83	105.75
VHF-Mid	98 A-1*	108-114	109.25	112.83	113.75
	99 A-2*	114-120	115.25	118.83	119.75
	14 A	120-126	121.25	124.83	125.75
	15 B	126-132	127.25	130.83	131.75
	16 C	132-138	133.25	136.83	137.75
	17 D	138-144	139.25	142.83	143.75
	18 E	144-150	145.25	148.83	149.75
	19 F	150-156	151.25	154.83	155.75
	20 G	156-162	157.25	160.83	161.75
	21 H	162-168	163.25	126.83	167.75
	22 I	168-174	169.25	172.83	173.75
VHF-High	7	174-180	175.25	178.83	179.75
	8	180-186	181.25	184.83	185.75
	9	186-192	187.25	190.83	191.75
	10	192-198	193.25	196.83	197.75
	11	198-204	199.25	202.83	203.75
	12	204-210	205.25	208.83	209.75
	13	210-216	211.25	214.83	215.75

* FCC Required +/- 25 KHz off-set.

VHF TELEVISION CHANNELS CON'T.

Table A.3 (con't)

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
VHF-Super con't	23 J	216-222	217.25	220.83	221.75
	24 K*	222-228	223.25	226.83	227.75
	25 L*	228-234	229.25	232.83	233.75
	26 M*	235-240	235.25	238.83	239.75
	27 N*	240-246	241.25	344.83	245.75
	28 O*	246-252	247.25	250.83	251.75
	29 P*	252-258	253.25	256.83	257.75
	30 Q*	258-264	259.25	262.83	263.75
	31 R*	264-270	249.25	268.83	269.75
	32 S*	270-276	271.25	274.83	275.75
	33 T*	276-282	277.25	280.83	281.75
	34 U*	282-288	283.25	286.83	287.75
	35 V*	288-294	289.25	292.83	293.75
	36 W*	294-300	295.25	298.83	299.75

* FCC Required +/- 12 KHz off-set.

UHF TELEVISION CHANNELS

Table A.4

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
UHF-Hyper	37 AA*	300-306	301.25	304.83	305.75
	38 BB*	306-312	307.25	310.83	311.75
	39 CC*	312-318	313.25	316.83	317.75
	40 DD*	318-324	319.25	322.83	323.75
	41 EE*	324-330	325.25	328.83	329.75
	42 FF*	330-336	331.25	334.83	335.75
	43 GG*	336-342	337.25	340.83	341.75
	44 HH*	342-348	343.25	346.83	347.75
	45 II*	348-354	349.25	352.83	353.75
	46 JJ*	354-360	355.25	358.83	359.75
	47 KK*	360-366	361.25	364.83	365.75
	48 LL*	366-372	367.25	370.83	371.75
	49 MM*	372-378	373.25	376.83	377.75
	50 NN*	378.384	379.25	382.83	383.75
	51 OO*	384-390	385.25	288.83	389.75
	52 PP*	390-396	391.25	394.83	395.75
	53 QQ*	396-402	397.25	400.83	401.75
	54 RR	402-408	403.25	406.83	407.75
	55 SS	408-414	408.25	412.83	413.75
	56 TT	414-420	415.25	418.83	419.75
	57 UU	420-426	421.25	424.83	425.75
	58 VV	426-432	427.25	430.83	431.75
	59 WW	432-438	433.25	436.83	437.75
	60 XX	438-444	439.25	442.83	443.75
	61 YY	444-450	445.25	448.83	449.75
	62 ZZ	450-456	451.25	454.83	455.75
	63 AAA	456-462	457.25	460.83	461.75
	64 BBB	462-468	463.25	466.83	467.75
	65 CCC	468-474	469.25	472.83	473.75
	66 DDD	474-480	475.25	478.83	479.75
	67 EEE	480-486	481.25	484.83	485.75
	68 FFF	486-492	487.25	490.83	491.75
	69 GGG	492-498	493.25	496.83	497.75
	70 HHH	498-504	499.25	502.83	503.75
	71 III	504-510	505.25	508.83	509.75
	72 JJJ	510-516	511.25	514.83	515.75
	73 KKK	516-522	517.25	520.83	521.75
	74 LLL	522-528	523.25	526.83	557.75
	75 MMM	528-534	529.25	532.83	533.75
	76 NNN	534-540	535.25	538.83	539.75
	77 OOO	540-546	541.25	544.83	545.75
	78 PPP	546-552	547.25	550.83	551.75
	79 QQQ	552-558	553.25	556.83	557.75
	80 RRR	558-564	559.25	562.83	563.75

* FCC Required +/- 12 KHz off-set.

UHF TELEVISION CHANNELS CON'T

Table A.4 (con't)

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
UHF-Hyper	81 SSS	564-570	565.25	568.83	569.75
	82 TTT	570-576	571.25	574.83	575.75
	83 UUU	576-582	577.25	580.83	581.75
	84 VVV	582-588	583.25	586.83	587.75
	85 WWW	588-594	589.25	592.83	593.75
	86 XXX	594-600	595.25	598.83	599.75
	87 YYY	600-606	601.25	604.83	605.75
	88 ZZZ	606-612	607.25	610.83	611.75
	89	612-618	613.25	616.83	617.75
	90	618-624	619.25	622.83	623.75
	91	624-630	625.25	628.83	629.75
	92	630-636	631.25	634.83	635.75
	93	636-642	637.25	640.83	641.75
	94	642-648	643.25	646.83	647.75
	100	648-654	649.25	652.83	653.75
	101	654-660	655.25	658.83	659.75
	102	660-666	661.25	664.83	665.75
	103	666-672	667.25	670.83	671.75
	104	672-678	673.25	676.83	677.75
	105	678-684	679.25	682.83	683.75
	106	684-690	685.25	688.83	689.75
	107	690-696	691.25	694.83	695.75
	108	696-702	697.25	700.83	701.75
	109	702-708	703.25	706.83	707.75
	110	708-714	709.25	712.83	713.75
	111	714-720	715.25	718.83	719.75
	112	720-726	721.25	724.83	725.75
	113	726-732	727.25	730.83	731.75
	114	732-738	733.25	736.83	737.75
	115	738-744	739.25	742.83	733.75
	116	744-750	745.25	748.83	749.75
	117	750-756	751.25	754.83	755.75
	118	756-762	757.25	760.83	761.75
	119	762-768	763.25	766.83	767.75
	120	768-774	769.25	772.83	773.75
	121	774-780	775.25	778.83	779.75
	122	780-786	781.25	784.83	785.75
	123	786-792	787.25	790.83	791.25

UHF TELEVISION CHANNELS CON'T

Table A.4 (con't)

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
UHF-Hyper	124	792-798	793.25	796.83	797.75
	125	798-804	799.25	802.83	803.75
	126	804-810	805.25	808.83	809.75
	127	810-816	811.25	814.83	815.75
	128	816-822	817.25	820.83	821.75
	129	822-828	823.25	826.83	827.75
	130	828-834	829.25	832.83	833.75
	131	834-840	835.25	838.83	839.75
	132	840-846	841.25	844.83	845.75
	133	846-852	847.25	850.83	851.75
	134	852-858	853.25	856.83	857.75
	135	858-864	859.25	862.83	863.75
	136	864-870	865.25	868.83	869.75
	137	870-876	871.25	874.83	875.75
	138	876-882	877.25	880.83	881.75
	139	882-888	883.25	886.83	887.75
	140	888-894	889.25	892.83	893.75
	141	894-900	895.25	898.83	899.75
	142	900-906	901.25	904.83	905.75
	143	906-912	907.25	910.83	911.75
	144	912-918	913.25	916.83	917.75
	145	918-924	919.25	922.83	923.75
	146	924-930	925.25	928.83	929.75
	147	930-936	931.25	934.83	935.75
	148	936-942	937.25	940.83	941.75
	149	942-948	943.25	946.83	947.75
	150	948-954	949.25	952.83	953.75
	151	954-960	955.25	958.83	959.75
	152	960-966	961.25	964.83	965.75
	153	966-972	967.25	970.83	971.75
	154	972-978	973.25	976.83	977.75
	155	978-984	979.25	982.83	983.75
	156	984-990	985.25	988.83	989.75
	157	990-996	991.25	994.83	995.75
	158	996-1002	997.25	1000.83	1001.75

UHF BROADCAST CHANNELS

Table A.5

Channel	Channel Limits	— Carrier Frequencies — (MHz) Visual	Color	Aural
14	470-476	471.25	474.83	475.75
15	476-482	477.25	480.83	481.75
16	482-488	483.25	486.83	487.75
17	488-494	489.25	492.83	493.75
18	494-500	495.25	498.83	499.75
19	500-506	501.25	504.83	505.75
20	506-512	507.25	510.83	511.75
21	512-518	513.25	516.83	517.75
22	518-524	519.25	522.83	523.75
23	524-530	525.25	528.83	529.75
24	530-536	531.25	534.83	535.75
25	536-542	537.25	540.83	541.75
26	542-548	543.25	546.83	547.75
27	548-554	549.25	552.83	553.75
28	554-560	555.25	558.83	559.75
29	560-566	561.25	564.83	565.75
30	566-572	576.25	570.83	571.75
31	572-578	573.25	576.83	577.75
32	578-584	579.25	582.83	583.75
33	584-590	585.25	588.83	589.75
34	590-596	591.25	594.83	595.75
35	596-602	597.25	600.86	601.75
36	602-608	603.25	606.83	607.75
37	608-614	609.25	612.83	613.75
38	614-620	615.25	618.83	619.75
39	620-626	621.25	624.83	625.74
40	626-632	627.25	630.83	631.75
41	632-638	633.25	636.83	637.75
42	638-644	639.25	642.83	643.75
43	644-650	645.25	648.83	649.75
44	650-656	651.25	654.83	655.75
45	656-662	657.25	660.83	661.75
46	662-668	663.25	666.83	667.75
47	668-674	669.25	672.83	673.75
48	674-680	675.25	678.83	679.75

UHF BROADCAST CHANNELS CON'T

Table A.5 (con't)

Channel	Channel Limits	— Carrier Frequencies — (MHz) Visual	Color	Aural
49	680-686	681.25	684.83	685.75
50	686-692	687.25	690.83	691.75
51	692-698	693.25	696.83	697.75
52	698-704	699.25	702.83	703.75
53	704-710	705.25	708.83	709.75
54	710-716	711.25	714.83	715.75
55	716-722	717.25	720.83	721.75
56	722-728	723.25	726.83	727.75
57	728-734	729.25	732.83	733.75
58	734-740	735.25	738.83	739.75
59	740-746	741.25	744.83	745.75
60	746-752	747.25	750.83	751.75
61	752-758	753.25	756.83	757.75
62	758-764	759.25	762.83	763.75
63	764-770	765.25	768.83	769.75
64	770-776	771.25	774.83	775.75
65	776-782	777.25	780.83	781.75
66	782-788	783.25	786.83	787.75
67	788-794	789.25	792.83	793.75
68	794-800	795.25	798.83	799.75
69	800-806	801.25	804.83	805.75
70*	806-812	807.25	810.83	811.75
71*	812-818	813.25	816.83	817.75
72*	818-824	819.25	822.83	823.75
73*	824-830	825.25	828.83	829.75
74*	830-836	831.25	834.83	935.75
75*	836-842	837.25	840.83	841.75
76*	842-848	843.25	846.83	847.75
77*	848-854	849.25	852.83	853.75
78*	854-860	855.25	858.83	859.75
79*	860-866	861.25	864.83	865.75
80*	866-872	867.25	870.83	871.75
81*	872-878	873.25	876.83	877.75
82*	878-884	879.25	882.83	883.75
83*	884-890	885.25	888.83	889.75

*These frequencies, formerly allocated to television broadcasting, have been allocated to cellular telephone. Reallocation of additional channels in the future is possible.

HRC TELEVISION CHANNELS

Table A.6

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
VHF Low	2	52.75-45.75	54	57.58	58.50
	3	58.75-64.75	60	63.58	64.50
	4	64.75-70.75	66	69.58	70.50
	5	76.75-82.75	78	81.58	82.50
	6	82.75-88.75	84	87.58	88.50
FM (Pseudo)	95 A-5	88.75-94.75	90	93.58	94.50
	96 A-4	94.75-100.75	96	99.58	100.50
	97 A-3	100.75-106.75	102	102.58	106.50
VHF Midband	98 A-2	106.75-112.75	108	111.58	112.50
	99 A-1	112.75-118.75	114	117.58	118.50
	14 A	118.75-124.75	120	123.58	124.50
	15 B	124.75-130.75	126	129.58	130.50
	16 C	130.75-136.75	132	135.58	136.50
	17 D	136.75-142.75	138	141.58	142.50
	18 E	142.75-148.75	144	147.58	148.50
	19 F	148.75-154.75	150	153.58	154.50
	20 G	154.75-160.75	156	159.58	160.50
	21 H	160.75-166.75	162	165.58	166.50
	22 I	166.75-172.75	168	171.58	172.50
VHF Highband	7	172.75-178.75	174	177.58	178.50
	8	178.75-184.75	180	183.58	184.50
	9	184.75-190.75	186	189.58	190.50
	10	190.75-196.75	192	195.58	196.50
	11	196.75-202.75	198	201.58	202.50
	12	202.75-208.75	204	207.58	208.50
	13	208.75-214.75	210	213.58	214.50
VHF Superband	23 J	214.75-220.75	216	219.58	220.50
	24 K	220.75-226.75	222	225.58	226.50
	25 L	226.75-232.75	228	231.58	232.50
	26 M	232.75-238.75	234	237.58	238.50
	27 N	238.75-244.75	240	243.58	244.50
	28 O	244.75-250.75	246	249.58	250.50
	29 P	250.75-256.75	252	255.58	256.50
	30 Q	256.75-262.75	258	261.58	262.50
	31 R	262.75-268.75	264	267.58	268.50
	32 S	268.75-274.75	270	273.58	274.50
	33 T	274.75-280.75	276	279.58	280.50
	34 U	280.75-286.75	282	285.58	286.50
	35 V	286.75-292.75	288	291.58	292.50
	36 W	292.75-298.75	294	297.58	298.50

HRC TELEVISION CHANNELS CON'T

Table A.6

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
UHF Hyper	37 AA	298.75-304.75	300	303.58	304.50
	38 BB	304.75-310.75	306	309.58	310.50
	39 CC	310.75-316.75	312	315.58	316.50
	40 DD	316.75-322.75	318	321.58	322.50
	41 EE	322.75-328.75	324	327.58	328.50
	42 FF	328.75-334.75	330	333.58	334.50
	43 GG	334.75-340.75	336	339.58	340.50
	44 HH	340.75-346.75	342	348.58	346.50
	45 II	346.75-352.75	348	351.58	352.50
	46 JJ	352.75-358.75	354	357.58	358.50
	47 KK	358.75-364.75	360	363.58	364.50
	48 LL	364.75-370.75	366	369.58	370.50
	49 MM	370.75-376.75	372	375.58	376.50
	50 NN	376.75-382.75	378	381.58	382.50
	51 OO	382.75-388.75	384	387.58	388.50
	52 PP	388.75-394.75	390	393.58	394.50
	53 QQ	394.75-400.75	396	399.58	400.50
	54 RR	400.75-406.75	402	405.58	406.50
	55 SS	406.75-412.75	408	411.58	412.50
	56 TT	412.75-418.75	414	417.58	418.50
	57 UU	418.75-424.75	420	423.58	424.50
	58 VV	424.75-430.75	426	429.58	430.50
	59 WW	430.75-436.75	432	435.58	436.50
	60 XX	436.75-442.75	438	441.58	442.50
	61 YY	442.75-448.75	444	447.58	448.50
	62 ZZ	448.75-454.75	450	453.58	454.50
	63 AAA	454.75-460.75	456	459.58	460.50
	64 BBB	460.75-466.75	462	465.58	466.50
	65 CCC	466.75-472.75	468	471.58	472.50
	66 DDD	472.75-478.75	474	477.58	478.50
	67 EEE	478.75-484.75	480	483.58	484.50
	68 FFF	484.75-490.75	486	489.58	490.50
	69 GGG	490.75-496.75	492	495.58	496.50
	70 HHH	496.75-502.75	498	501.58	502.50
	71 III	502.75-508.75	504	507.58	508.50
	72 JJJ	508.75-514.75	510	513.58	514.50
	73 KKK	514.75-520.75	516	519.58	520.50
	74 LLL	520.75-526.75	522	525.58	526.50
	75 MMM	526.75-532.75	528	531.58	532.50
	76 NNN	532.75-538.75	534	537.58	538.50
	77 OOO	538.75-544.75	540	543.58	544.50
	78 PPP	544.75-550.75	546	549.58	550.50
	79 QQQ	550.75-556.75	552	555.58	556.50
	80 RRR	556.75-562.75	558	561.58	562.50
	81 SSS	562.75-568.75	564	567.58	568.50
	82 TTT	568.75-574.75	570	573.58	574.50
	83 UUU	574.75-580.75	576	579.58	580.50
	84 VVV	580.75-586.75	582	585.58	586.50
	85 WWW	586.75-592.75	588	591.58	592.50

HRC TELEVISION CHANNELS CON'T

Table A.6

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
UHF Hyper	86 XXX	592.75-598.75	594	597.58	598.50
	87	598.75-604.75	600	603.58	604.50
	88	604.75-610.75	606	609.58	610.50
	89	610.75-616.75	612	615.58	616.50
	90	616.75-622.75	618	621.58	622.50
	91	622.75-628.75	624	627.58	628.50
	92	628.75-634.75	630	633.58	634.50
	93	634.75-640.75	636	639.58	640.50
	94	640.75-646.75	642	645.58	646.50
	100	646.75-652.75	648	651.58	652.50
	101	652.75-658.75	654	656.58	658.50
	102	658.75-664.75	660	662.58	664.50
	103	664.75-670.75	666	668.58	670.50
	104	670.75-676.75	672	674.58	676.50
	105	676.75-682.75	678	680.58	682.50
	106	682.75-688.75	684	686.58	688.50
	107	688.75-694.75	690	692.58	694.50
	108	694.75-700.75	696	698.58	700.50
	109	700.75-706.75	702	704.58	706.50
	110	706.75-712.75	708	710.58	712.50
	111	712.75-718.75	714	716.58	718.50
	112	718.75-724.75	720	722.58	724.50
	113	724.75-730.75	726	728.58	730.50
	114	730.75-736.75	732	734.58	736.50
	115	736.75-742.75	738	740.58	742.50
	116	742.75-748.75	744	746.58	748.50
	117	748.75-754.75	750	752.58	754.50
	118	754.75-760.75	756	758.58	760.50
	119	760.75-766.75	762	764.58	766.50
	120	766.75-772.75	768	770.58	772.50
	121	772.75-778.75	774	776.58	778.50
	122	778.75-784.75	780	782.58	784.50
	123	784.75-790.75	786	788.58	790.50
	124	790.75-796.75	792	794.58	796.50
	125	796.75-802.75	798	800.58	802.50
	126	802.75-808.75	804	806.58	808.50
	127	808.75-814.75	810	812.58	814.50
	128	814.75-820.75	816	818.58	820.50
	129	820.75-826.75	822	824.58	826.50
	130	826.75-832.75	828	830.58	832.50
	131	832.75-838.75	834	836.58	838.50
	132	838.75-844.75	840	842.58	844.50
	133	844.75-850.75	846	848.58	850.50
	134	850.75-856.75	852	854.58	856.50
	135	856.75-862.75	858	860.58	862.59
	136	862.75-868.75	864	866.58	868.50
	137	868.75-874.75	870	872.58	874.50
	138	874.75-880.75	876	878.58	880.50

HRC TELEVISION CHANNELS CON'T

Table A.6

Band	Channel	Channel Limits	-Carrier Frequencies (MHz) - Visual	Color	Aural
UHF Hyper	139	880.75-886.75	882	884.58	886.50
	140	886.75-892.75	888	890.58	892.50
	141	892.75-898.75	894	896.58	898.50
	142	898.75-904.75	900	902.58	904.50
	143	904.75-910.75	906	908.58	910.50
	144	910.75-916.75	912	914.58	916.50
	145	916.75-922.75	918	920.58	922.50
	146	922.75-928.75	924	926.58	928.50
	147	928.75-934.75	930	932.58	934.50
	148	934.75-940.75	936	938.58	940.50
	149	940.75-946.75	942	944.58	946.50
	150	946.75-952.75	948	950.58	952.50
	151	952.75-958.75	954	956.58	958.50
	152	958.75-964.75	960	962.58	964.50
	153	964.75-970.75	966	968.58	970.50
	154	970.75-976.75	972	974.58	976.50
	155	976.75-982.75	978	980.58	982.50
	156	982.75-988.75	984	986.58	988.50
	157	988.75-994.75	990	992.58	994.50
	158	994.75-1000.75	996	998.58	1000.50

FM RADIO CHANNELS

Table A.7

Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
201	88.1	235	94.9	269	101.7
202	88.3	236	95.1	270	101.9
203	88.5	237	95.3	271	102.1
204	88.7	238	95.5	272	102.3
205	88.9	239	95.7	273	102.5
206	89.1	240	95.9	274	102.7
207	89.3	241	96.1	275	102.9
208	89.5	242	96.3	276	103.1
209	89.7	243	96.5	277	103.3
210	89.9	244	96.7	278	103.5
211	90.1	245	96.9	279	103.7
212	90.3	246	97.1	280	103.9
213	90.5	247	97.3	281	104.1
214	90.7	248	97.5	282	104.3
215	90.9	249	97.7	283	104.5
216	91.1	250	97.9	284	104.7
217	91.3	251	98.1	285	104.9
218	91.5	252	98.3	286	105.1
219	91.7	253	98.5	287	105.3
220	91.9	254	98.7	288	105.5
221	92.1	255	98.9	289	105.7
222	92.3	256	99.1	290	105.9
223	92.5	257	99.3	291	106.1
224	92.7	258	99.5	292	106.3
225	92.9	259	99.7	293	106.5
226	93.1	260	99.9	294	106.7
227	93.3	261	100.1	295	106.9
228	93.5	262	100.3	296	107.1
229	93.7	263	100.5	297	107.3
230	93.9	264	100.7	298	107.5
231	94.1	265	100.9	299	107.7
232	94.3	266	101.1	300	107.9
233	94.5	267	101.3		
234	94.7	268	101.5		

Appendix B
Engineering Formulas

SIGNAL LEVELS (dBmV)

dBmV = 20 log (E / 0.001 volts)

with Z = 75-ohms

POWER LEVELS (dBm)

dBm = 10 log (P / 0.001W)

POWER LEVELS (dBW)

dBW = 10 log (P / 1 watt)

CONVERSION FORMULAS

$$dBmV = dBm + 49.75$$

$$dBm = dBmV - 49.75$$

DECIBEL FORMULAS

For Equal Impedances ($Z_1 = Z_2$)

$$dB = 10 \log P_1 / P_2$$

$$= 20 \log E_1 / E_2$$

$$= 20 \log I_1 / I_2$$

For Unequal Impedances

$$dB = 10 \log P_1 / P_2$$

$$= 20 \log (E_1 Z_2^{1/2} / E_2 Z_1^{1/2})$$

$$= 20 \log (I_1 Z_1^{1/2} / I_2 Z_2^{1/2})$$

LAW OF LOGARITHMS

$\log_a x\,y = \log_a x + \log_a y$

$\log_a x/y = \log_a x - \log_a y$

$\log_a x^r = r \log x$

CARRIER-TO-NOISE RATIO (C/N)

C/N = Output + 59.2 - NF - Gain, where:

Output = signal output (dBmV)

59.2 = external noise floor,

NF = noise figure (dB), and

Gain = amplifier gain (dB)

Appendix C
World Wide Broadcast Formats

International Channel Formats

Table C-1

Broadcast System	Lines	Bandwidth (MHz)	Audio Separation (MHz)	Audio Modulation	Field Frequency Lines (Hz)
A	405	5	3.5	FM	50/10125
B	625	7	5.5	FM	50/15625
C	625	7	5.5	AM	50/15625
D	625	8	6.5	FM	50/15625
E	819	14	11.15	AM	50/20475
G/H	625	8	5.5	FM	50/15625
I	625	8	6.0	FM	50/15625
K/K1	625	8	6.5	FM	50/15625
L	625	8	6.5	AM	50/15625
M	525	6	4.5	FM	60/15750
N	625	6	4.5	FM	50/15625

The location of the color carrier depends on the channel format.

Format	Color carrier frequency*
NTSC	+ 3.58 MHz
PAL	+ 4.43 MHz
SECAM	+ 4.43 MHz

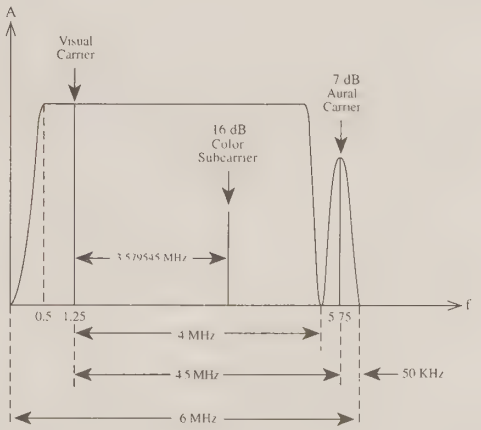
*** Relative to the video carrier frequency**

International Channel Formats con't

Table C-1

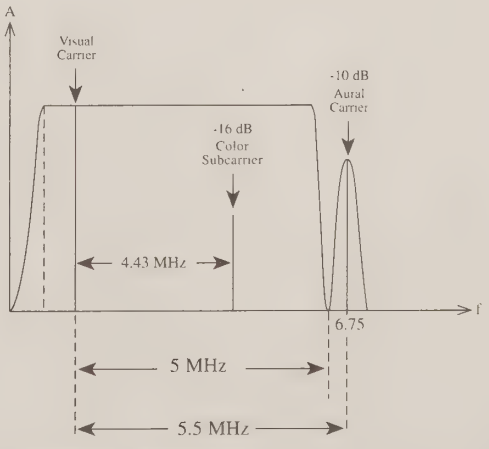
NTSC TELEVISION CHANNEL
6 MHz (M, N)

Figure C-1



PAL TELEVISION CHANNEL
7 MHz (B, C)

Figure C-2

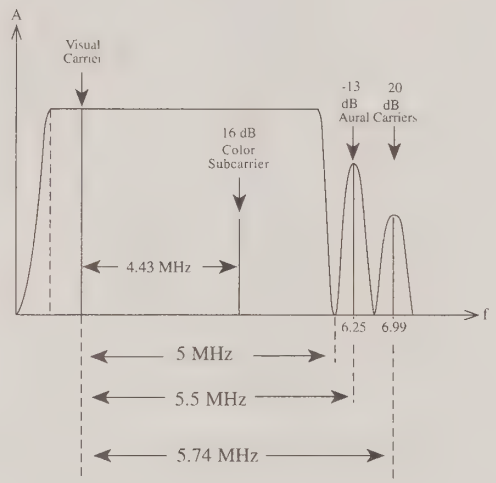


International Channel Formats con't

Table C-1

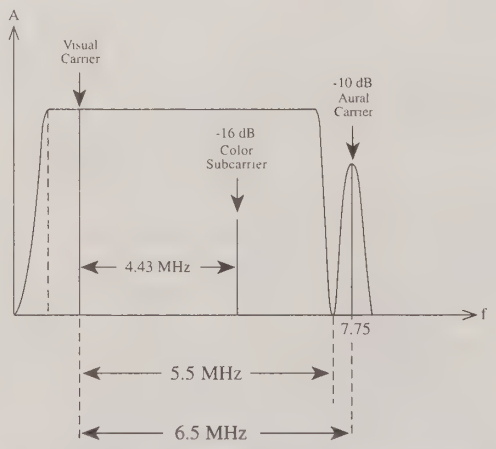
PAL TELEVISION CHANNEL
8 MHz (G Dual Sound)

Figure C-3



PAL TELEVISION CHANNEL
8 MHz (P, K/K1, L)

Figure C-4

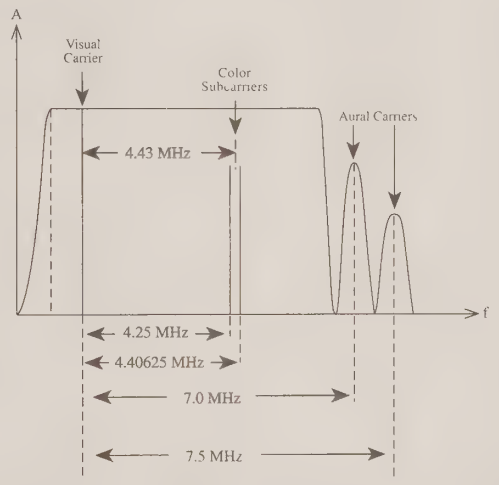


International Channel Formats con't

Table C-1

SECAM TELEVISION CHANNEL
8 MHz (625 lines)

Figure C-5



INTERNATIONAL TV FORMATS

Table C-2

	- VHF System -			- UHF System -			
Country	Broadcast	Color	Channel Layout	Broadcast	Color	Channel Layout	Voltage Line Frequency
Afghanistan	B	PAL	CCIR		SECAM		220-50
Albania	B	PAL	CCIR	G	PAL G	CCIR	220-50
Algeria	B	PAL	CCIR		PAL G		127/220/380-50
Andorra							220-50
Angola	I	PAL	CCIR				220-50
Anguilla							110-50
Antigua	M	NTSC	USA				110-50
Argentina	N	PAL*	USA		PAL		220-50
Ascension Island							220-50
Australia	B	PAL	Unique		PAL		240/415-50
Austria	B	PAL	CCIR	G	PAL	CCIR	220/380-50
Azores	B	PAL	CCIR				220-50
Bahamas	M	NTSC	USA				110/220-60
Bahrain	B	PAL	CCIR		PAL		230-50
Bangladesh	B	PAL	CCIR				220/440-50
Barbados	M	NTSC	USA				110/220-50
Barbuda	M	NTSC	USA				110/220-50
Belgium	B	PAL	CCIR	H	PAL	CCIR	220-50
Belau							220-50
Belize							110/220-60
Benin	K		CCIR				220/380-50
Bermuda	M	NTSC	USA				115/230-60
Bhutan							220-50
Bolivia	M	NTSC	USA	N	NTSC	USA	110/220-50
Brazil	M	PAL	USA				110/127/220-50/60
Brunei	B	PAL	CCIR				110/127/220-50/60
Bulgaria	D	SECAM	CCIR	K	SECAM	ORIT(R)	220-50
Burma	D	SECAM					230-50
Burundi	K1	SECAM					220/380-50
Cambodia	M	NTSC					230/380-50
Cameroon		PAL		PAL B			220/230-50
Canada	M	NTSC	USA				115/230-60
Canary Islands	B	PAL	CCIR				110/220-50
Canton Island							110/220-60
Cape Verde Island							110/220-60
Cayman Islands							110-60
Central Africa Rep.							220-50
Chad	K1			SECAM			220-50
Chile	M	NTSC	USA				220/380-50
Christmas Island							220-50

* -3.58 MHz Color Subcarrier

INTERNATIONAL TV FORMATS

Table C-2 con't

	- VHF System -			- UHF System -			
Country	Broadcast	Color	Channel Layout	Broadcast	Color	Channel Layout	Voltage Line Frequency
China	D	PAL	Unique				220-50
C.I.S.	D	SECAM	OIRT(R)	K	SECAM	CCIR	127/220-50
Colombia	M	NTSC	USA				115/220-60
Comoro Islands							220-50
Congo	D		CCIR				220-50
Cocos Islands							220-50
Cook Islands							220-50
Costa Rica	M	NTSC	USA				120/220-60
Cuba	M	NTSC	USA				115/220-60
Cyprus	G	PAL	CCIR	G	PAL	CCIR	240-50
Czech Republic	D	SECAM	ORIR(R)	K	SECAM	CCIR	220-50
Denmark	B	SECAM	USA	G			110/220-60
Djibouri	B	SECAM	FOTU	G	SECAM		220-50
Dominicas							240-50
Dominican Republic	M	NTSC	USA	M			110-60
Dubai (UAE)	B	PAL	CCIR	G	PAL	CCIR	220-50
Ecuador	M	NTSC	USA	M	NTSC		110/220-60
Egypt	B	SECAM	CCIR	G	SECAM		127/220-50
El Salvador	M	NTSC	USA	M	NTSC		110/220-60
Ethiopia	B	PAL	CCIR	G	PAL		127/220-50
Falkan Islands	B	PAL					220-50
Faroe Islands	B	PAL	CCIR				220-50
Fiji	B	PAL					240-50
Finland	B	PAL	CCIR	G	PAL	CCIR	220/380-50
France	L	SECAM	Unique	L	SECAM	CCIR	various-50
Gabon	K1	SECAM	FOTU				220-50
Gambia	I	PAL I					230-50
Germany	B	PAL	OIRT(R)	G	PAL		220/380-5
Ghana	G	PAL	CCIR	G	PAL		230-50
Gibraltar	B	PAL	CCIR	H			240-50
Greece	B	SECAM	CCIR	G	PAL	CCIR	220-50
Greenland	B	PAL	CCIR				220/380-50
Greenland (AFRTS)	M	NTSC	USA				110/220-60
Grenada							220-50
Guadeloupe	K1	SECAM	FOT.				220-50
Guam	M	NTSC	USA				110/220-60
Guatemala	M	NTSC	USA	M	NTSC		110/220/127/220-60
Guyana	K	SECAM					220-50
Guiana-French	K1	SECAM	FOTU				220/380-50
Guinea-Republic	K	PAL	FOTU				220/380-50
Guinea-Bissau							220/380-50

INTERNATIONAL TV FORMATS

Table C-2 con't

	- VHF System -			- UHF System -			
Country	Broadcast	Color	Channel Layout	Broadcast	Color	Channel Layout	Voltage Line Frequency
Guinea-Equatorial	B		CCIR				220/380-50
Haiti	M	NTSC	USA				110/220-50/60
Holland	B	PAL	CCIR	G	PAL	CCIR	220-50
Honduras	M	NTSC	USA	M	NTSC		110-60
Hong Kong	I	PAL	CCIR			CCIR	200-50
Hungary	D	SECAM	OIRT(R)	K	PAL		220-50
Iceland	B	PAL	CCIR				220-50
India	B	PAL	CCIR				230/400-50
Indonesia	B	PAL	CCIR	G	PAL		127/220-50
Iran	B	SECAM	CCIR	G	SECAM		220-50
Iraq	B	SECAM	CCIR				220/380-50
Ireland	I	PAL	Unique	I	PAL	Unique	220/380-50
Israel	B	PAL	CCIR	G	PAL	CCIR	230/400-50
Italy	B	PAL	Unique	G	PAL	CCIR	220/380-50
Ivory Coast	K1	SECAM	FOTU				220/380-50
Jamaica	M	NTSC	USA				110/220-50
Japan	M	NTSC	Unique	M	NTSC	Unique	110/220-50/60
Johnson Island	M	NTSC	USA				110/220-60
Jordan	B	PAL	CCIR	G	PAL	CCIR	220-50
Kampuchea							120/208/220-50
Kenya	B	PAL	CCIR	G	PAL		240-50
Kiribati							240-50
Korea (South)	M	NTSC	USA				110/60
Korea (North)	D	SECAM	Unique				220-50
Kuwait	B	PAL	CCIR				240-50
Laos	M		USA				127/220-50
Lebanon	B	SECAM	CCIR	G	SECAM		110/190-50
Liberia	B	PAL	CCIR				120-60
Libya	B	SECAM	CCIR	G	SECAM		127/130-50
Luxembourg	B	PAL	CCIR	G/L	SECAM	CCIR	110/220-50
Macau							110/220-50
Madeira	B	PAL	CCIR				220/380-50
Madagascar	K1	SECAM	FOTU				110/220-50
Malawi	B	PAL		G	PAL		230-50
Malaysia (Peninsula)	B	PAL	CCIR				230/400-50
Mali	K1	SECAM					220-50
Maldives	B	PAL					220-50
Malta	B	PAL	CCIR	H	PAL	CCIR	240-50
Martinique	K1	SECAM	FOT				220/380-50
Marshall Islands							110/220-60
Mauritania	B	SECAM	FOT				220/380-50

INTERNATIONAL TV FORMATS

Table C-2 con't

	- VHF System -			- UHF System -			
Country	Broadcast	Color	Channel Layout	Broadcast	Color	Channel Layout	Voltage Line Frequency
Mauritius	B	SECAM	CCIR				240-50
Mayotte							220-50
Mexico	M	NTSC	USA				110/220-60
Midway Islands	M	NTSC	USA				110/220-60
Micronesia	M	NTSC					
Monaco	L	SECAM	CCIR			CCIR	127/220-50
Mongolia	D	SECAM	OIRT				220-50
Monserrat							220-50
Morocco	B	SECAM	Unique				127/220/50
Mozambique	B	PAL	CCIR				220-50
Namibia	I	PAL	Unique				220-50
Nauru							220-50
Nepal	B	PAL					220-50
Netherland Antilles	M	NTSC		M	NTSC		127/220-50-60
Netherlands	B	PAL	CCIR	G	PAL	CCIR	220-50
New Caledonia	K1	SECAM	FOT				220-50
New Hebrides							220-50
New Guinea	B	PAL		G	PAL		220/380-50
New Zealand	B	PAL	Unique	G	PAL		230/400-50
Nicaragua	M	NTSC		M	NTSC		
Niger	K1	SECAM	FOT				220/38--50
Nigeria	B	PAL	CCIR	G	PAL	CCIR	230/400-50
Niue Island							220-50
North Mariana Island	M	NTSC	USA				110/220-60
Norfolk Island							220-50
Norway	B	PAL	CCIR	G	PAL	CCIR	230-50
Oman	B	PAL	CCIR	G	PAL	CCIR	220-50
Pakistan	B	PAL	CCIR				230/400-50
Panama	M	NTS C	USA				110/115/120/126-60
Papua New Guinea							240/415-50
Paraguay	N	PAL N	CCIR				220-50
Peru	M	NTSC	USA	M	NTSC		220-60
Phillippines	M	NTSC	USA	M	NTSC		110/220-60
Poland	D/K	SECAM	ORIT(E)	K	PAL	CCIR	220/380-50
Portugal	B	PAL	CCIR	G	PAL	CCIR	220/380-50
Puerto Rico	M	NTSC	USA				120-60
Qatar	B	PAL B	CCIR				220-50
Reunion	K1	SECAM	FOTU				220-50
Romania	D	PAL	OIRT(R)	K	PAL		220-50
Rwanda	K1	SECAM					220-50
Sabah/Sarawak	B	PAL					220-50

INTERNATIONAL TV FORMATS

Table C-2 con't

Country	- VHF System - Broadcast	Color	Channel Layout	- UHF System - Broadcast	Color	Channel Layout	Voltage Line Frequency
Samoa-American	M	NTSC	USA				230-50
Samoa-Western							230-50
SaoTome							220-50
Sarawak	B	PAL	CCIR				220-50
Saudi Arabia	B	SECAM	CCIR	G	SECAM	CCIR	127/220/380-50/60
Senegal	K1	SECAM	FOTU				127/220-50
Seychelles	B	PAL	CCIR	G	PAL		230-50
Sierra Leone	B	PAL	CCIR	G	PAL		230-50
Singapore	B	PAL	CCIR	G	PAL		230/400-50
Slovak Republic	D	SECAM	ORIR(R)	K	SECAM	CCIR	220-50
Society Islands	K		FOT				240-50
Solomon Islands							240-50
Somalia	B	PAL		G	PAL		230-50
South Africa	I	PAL	Unique	I	PAL		220/380-50
South West Africa							220/380-50
Spain	B	PAL	CCIR	G	PAL	CCIR	127/220/380-50
Sri Lanka	B	PAL	CCIR				220-50
St. Helena							220-50
St. Kitts	M	NTSC	USA				220/60
St. Pierre	K	SECAM	FOTU				220-50
Sudan	B	PAL	CCIR	G	PAL		240-50
Surinam	M	NTSC	USA	M	NTSC		110/115/127/220-60
Swaziland	B	PAL	CCIR	G	PAL	CCIR	230-50
Sweden	B	PAL	CCIR	G	PAL	CCIR	220/380-50
Switzerland	B	PAL	CCIR	G	PAL	CCIR	220/380-50
Syria	B	SECAM	CCIR				115/200-50
Tahiti	K1	SECAM	FOTU				127-60
Taiwan	M	NTSC	USA	M	NTSC		110/200-60
Tanzania	B	PAL	CCIR	B	PAL		230/440-50
Thailand	B	PAL B	CCIR				230/380-50
Trinidad	M	NTSC		M	NTSC		115/230-60
Tristan de Cunha							220-50
Togo	K1	SECAM	FOTU				127/220-50
Trust Territory	M	NTSC	USA				110/220-60
Tunisia	B	SECAM	CCIR				115/220/380-50
Turks-Caicos Islands	M	NTSC	USA				110/220/440-60
Turkey	B	PAL	CCIR	G	PAL		220/380-50
Tuvalu							220-50
Uganda	B	PAL	CCIR	G	PAL		240/415-50
United Arab Emirates	B	PAL	CCIR	G	PAL	CCIR	220-50
United Kingdom	A	PAL	Unique	I	PAL		240/415-50

INTERNATIONAL TV FORMATS

Table C-2 con't

	- VHF System -			- UHF System -			
Country	Broadcast	Color	Channel Layout	Broadcast	Color	Channel Layout	Voltage Line Frequency
U.S.A.	M	NTSC	USA	M	NTSC	USA	110/220-60
Upper Volta	K		FOTU				220/380-50
Uruguay	N	PAL	CCIR				220-50
Vatican State							220/380-50
Venezuela	M	NTSC	USA	M	NTSC		120/240-60
Vietnam	B	PAL	OIRT(R)	G	PAL		120/127/230-50
Virgin Islands	M	NTSC	USA				110-60
Wake Island	M	NTSC	USA				110/220-60
Yemen (South)	B	PAL	CCIR				230-50
Yemen (North)	B	NTSC	CCIR				230-50
Yugoslavia	B	PAL	CCIR	G	PAL	CCIR	220/380-50
Zaire	K1	SECAM	FOTU				220-50
Zambia	B	PAL	CCIR	G	PAL		220-50
Zimbabwe	B	PAL	CCIR	G	PAL		230/240-50

Appendix D
International TV Channels

AUSTRALIAN TV CHANNELS

PAL B

Table D-1

Band	Channel	Visual Carrier Frequency (MHz)	1st S Carrier Frequency (MHz)	2nd S Carrier Frequency (MHz)	Frequency Limits (MHz)
VHF I	0	46.25	51.75	51.992	45-52
	1	57.25	62.75	62.992	56-63
	2	64.25	69.75	69.992	63-70
VHF II (1)	3	86.25	91.75	91.992	85-92
	4	95.25	100.75	100.992	94-101
	5	102.25	107.75	107.992	101-108
	5A	138.25	143.75	143.992	137-144
VHF III	6	175.25	180.75	180.992	174-181
	7	182.25	187.75	187.992	181-188
	8	189.25	194.75	194.992	188-195
	9	196.25	201.75	201.992	195-202
	10	209.25	214.75	214.992	208-215
	11	216.25	221.75	221.992	215-222
UHF IV	28	527.25	532.75	532.992	526-533
	29	534.25	539.75	539.992	533-540
	30	541.25	546.75	546.992	540-547
	31	548.25	553.75	553.992	547-554
	32	555.25	560.75	560.992	554-561
	33	562.25	567.75	567.992	561-568
	34	569.25	574.75	574.992	568-575
	35	576.25	581.75	581.992	575-582
UHF V	36 (2)	583.25	588.75	588.992	582-589
	37 (2)	590.25	595.75	595.992	589-596
	38 (2)	597.25	602.75	602.992	596-603
	39 (3)	604.25	609.75	609.992	603-610
	40 (3)	611.25	616.75	616.992	610-617
	41	618.25	623.75	623.992	617-624
	42	625.25	630.75	630.992	624-631
	43	632.25	637.75	637.992	631-638
	44	639.25	644.75	644.992	638-645
	45	646.25	651.75	651.992	645-652
	46	653.25	658.75	658.992	652-659
	47	660.25	665.75	665.992	659-666
	48	667.25	672.75	672.992	666-673
	49	674.25	679.75	679.992	673-680
	50	681.25	686.75	686.992	680-687

AUSTRALIAN TV CHANNELS (con't)

PAL B

Band	Channel	Visual Carrier Frequency (MHz)	1st S Carrier Frequency (MHz)	2nd S Carrier Frequency (MHz)	Frequency Limits (MHz)
UHF V con't	51	688.25	693.75	693.992	687-694
	52	695.25	700.75	700.992	694-701
	53	702.25	707.75	707.992	701-708
	54	709.25	714.75	714.992	708-715
	55	716.25	721.75	721.992	715-722
	56	723.25	728.75	728.992	722-729
	57	730.25	735.75	735.992	729-736
	58	737.25	742.75	742.992	736-743
	59	744.25	749.75	749.992	743-750
	60	751.25	756.75	756.992	750-757
	61	758.25	763.75	763.992	757-764
	62	765.25	770.75	770.992	764-771
	63	772.25	777.75	777.992	771-778
	64	779.25	784.75	784.992	778-785
	65	786.25	791.75	791.992	785-792
	66	793.25	798.75	798.992	792-799
	67	800.25	805.75	805.992	799-806
	68	807.25	812.75	812.992	806-813
	69	814.25	819.75	819.992	813-820
	IF	38.90	33.40		33.15-40.15

BRITISH TV CHANNEL FREQUENCIES

STANDARD PAL I

Table D-2

BAND	CHANNEL NUMBER	BAND LIMITS (MHz)	VISUAL CARRIER FREQUENCY	AURAL CARRIER FREQUENCY
I	B1	41.25-46.25	45.00	41.50
	B2	48-53	51.75	48.25
	B3	53-58	56.75	53.25
	B4	58-63	61.75	58.25
	B5	63-68	66.75	63.25
III	B6	176-181	179.75	176.25
	B7	181-186	184.75	181.25
	B8	186-191	189.75	186.25
	B9	191-196	194.75	191.25
	B10	196-201	199.75	196.25
	B11	201-206	204.75	201.25
	B12	206-211	209.75	206.25
	B13	211-216	214.75	211.25
	B14	216-221	219.75	216.25

MAINLAND CHINA

Table D-3

BAND	CHANNEL	FREQUENCY RANGE (MHz)	VISUAL (MHz)	AURAL (MHz)
I	1	48.5 to 56.5	49.75	56.25
	2	56.5 to 64.5	57.75	64.25
	3	64.5 to 72.56	65.75	72.25
	4	76 to 84	77.25	83.75
	5	84 to 92	85.25	91.75
III	6	167 to 175	168.25	174.75
	7	175 to 183	176.25	182.75
	8	183 to 191	184.25	190.75
	9	191 to 199	192.25	198.75
	10	199 to 207	200.25	206.75
Standard D	11	207 to 215	208.25	214.75
	12	215 to 223	216.25	222.75
Standard K	13	470 to 478	471.25	477.75
	14	478 to 486	479.25	485.75
	15	486 to 494	487.25	493.75
	16	494 to 502	495.25	501.75
IV	17	502 to 510	503.25	509.75
	18	510 to 518	511.25	517.75
	19	518 to 526	519.25	525.75
	20	526 to 534	527.25	533.75
	21	534 to 542	535.25	541.75
	22	542 to 550	543.25	549.75
	23	550 to 558	551.25	557.75
	24	558 to 566	559.25	565.75
V	25	606 to 614	607.25	613.75
	26	614 to 622	615.25	621.75
	27	622 to 630	623.25	629.75
	28	630 to 638	631.25	637.75
	29	638 to 646	639.25	645.75
	30	646 to 654	647.25	653.75
	31	654 to 662	655.25	661.75
	32	662 to 670	663.25	669.75
	33	670 to 678	671.25	677.75
	34	678 to 686	679.25	685.75
	35	686 to 694	687.25	693.75
	36	694 to 702	695.25	701.75
	37	702 to 710	703.25	709.75
	38	710 to 718	711.25	717.75
	39	718 to 726	719.25	725.75
	40	726 to 734	727.25	733.75
	41	734 to 742	735.25	741.75
	42	742 to 750	743.25	749.75
	43	750 to 758	751.25	757.75
	44	758 to 766	759.25	765.75
	45	766 to 774	767.25	773.75
	46	774 to 782	775.25	781.75
	47	782 to 790	783.25	789.75
	48	790 to 798	791.25	797.75
	49	798 to 806	799.25	805.75
	50	806 to 814	807.25	813.75
	51	814 to 822	815.25	821.75
	52	822 to 830	823.25	829.75
	53	830 to 838	831.25	837.75
	54	838 to 846	839.25	845.75
	55	846 to 854	847.25	853.75
	56	854 to 862	855.25	861.75
	57	862 to 870	863.25	869.75
	58	870 to 878	871.25	877.75
	59	878 to 886	879.25	885.75
	60	886 to 894	887.25	893.75
	61	894 to 902	895.25	901.75
	62	902 to 910	903.25	909.75
	63	910 to 918	911.25	917.75
	64	918 to 926	919.25	925.75
	65	926 to 934	927.25	933.75
	66	934 to 942	935.25	941.75
	67	942 to 950	943.25	949.75
	68	950 to 958	951.25	957.75
	IF	30.25 - 38.25	37.00	30.50

EASTERN EUROPEAN TV CHANNEL FREQUENCIES

STANDARD PAL D

Table D-4

BAND	CHANNEL #	BAND (MHz)	VISUAL (MHz)	AURAL (MHz)
IF(c)	-	32.15-40.15	38.90	32.40
	R I	48.5-56.5	49.75	56.25
I	R II	58-66	59.25	66.75
	R III	76-84	77.25	77.25
	R IV	84-92	85.25	85.25
	R V	92-100	93.25	93.25
	R VI	174-182	175.25	175.25
	R VII	182-190	183.25	183.25
	R VIII	190-198	191.25	191.25
III	R IX	198-206	199.25	199.25
	R X	206-213	207.25	207.25
	R XI	214-222	215.25	215.25
	R XII	222-230	223.25	223.25

FRENCH OVERSEAS TV CHANNEL FREQUENCIES

STANDARD K1

Table D-5

BAND	CHANNEL #	BAND (MHz)	VISUAL (MHz)	AURAL (MHz)
IF	-	31.45-39.45	32.70	39.20
	4	174-182	175.25	181.75
	5	182-190	183.25	189.75
III	6	190-198	191.25	197.75
	7	198-206	199.25	205.75
	8	206-214	207.25	213.75
	9	214-222	215.25	221.75

FRENCH STANDARD TV CHANNEL FREQUENCIES

STANDARD PAL L

BAND	CHANNEL #	BAND (MHz)	VISUAL (MHz)	AURAL (MHz)
IF	-	31.45-39.45	32.70	39.20
	A	41-49	47.75	41.25
I	B	49-57	55.75	49.25
	C	57-65	63.75	57.25
	C 1	53.75-61.75	60.50	54.00
	1	174.75-182.75	176.00	182.50
	2	182.75-190.75	184.00	190.50
III	3	190.75-198.75	192.00	198.50
	4	198.75-206.75	200.00	206.50
	5	206.75-214.75	208.00	214.50
	6	214.75-222.75	216.00	222.50

FRENCH STANDARD TV CHANNEL FREQUENCIES

STANDARD PAL E

Table D-5 con't

BAND	CHANNEL #	BAND (MHz)	VISUAL (MHz)	AURAL (MHz)
IF	-	26.30-39.45	28.05	39.20
I	F 2	41.00-54.15	52.40	41.25
	F 4	54.15-67.30	65.55	54.40
III	F 5	162.25-175.15	164.00	175.15
	F 6	162.00-175.15	173.40	162.25
	F 7	175.40-188.55	177.15	188.30
	F 8A	174.00-188.00	185.25	174.10
	F 8	175.15-188.30	186.55	175.40
	F 9	188.55-201.70	190.30	201.45
	F 10	188.30-201.45	199.70	188.55
	F 11	201.70-214.85	203.45	214.60
	F 12	201.45-214.60	212.85	201.70

INTERNATIONAL CCIR UHF CHANNEL FREQUENCIES

STANDARD PAL G, H, I, K & L

Table D-6

BAND	CHANNEL NUMBER	BAND LIMITS (MHz)	VISUAL CARRIER	AURAL G, H	CARRIER I	FREQUENCY K, L
	IF - same as VHF IF in each corresponding country adopting					
	21	470-478	471.25	476.75	477.25	477.75
	22	478-486	479.25	484.75	485.25	485.75
	23	486-494	487.25	492.75	493.25	493.75
	24	494-502	495.25	500.75	501.25	501.75
	25	502-510	503.25	508.75	509.25	509.75
	26	510-518	511.25	516.75	517.25	517.75
	27	518-526	519.25	524.75	525.25	525.75
	28	526-534	527.25	532.75	533.25	533.75
	29	534-542	535.25	540.75	541.25	541.75
V	30	542-550	543.25	548.75	549.25	549.75
	31	550-558	551.25	556.75	557.25	557.75
	32	558-566	559.25	564.75	565.25	565.75
	33	566-574	567.25	572.25	573.25	573.75
	34	574-582	575.25	580.75	581.25	581.75
	35	582-590	583.25	588.75	589.25	589.75
	36	590-598	591.25	596.75	597.25	597.75
	37	598-606	599.25	604.75	605.25	605.75
	38	606-614	607.25	612.75	613.25	613.75
	39	614-622	615.25	620.75	621.25	621.75
	40	622-630	623.25	628.75	629.25	629.75
	41	630-638	631.25	636.75	637.25	637.75
	42	638-646	639.25	644.75	645.25	645.75
	43	646-654	647.25	652.75	653.25	653.75
	44	654-662	655.25	660.75	661.25	661.75
	45	662-670	663.25	668.75	669.25	669.75
	46	670-678	671.25	676.75	677.25	677.75
	47	678-686	679.25	684.75	685.25	685.75
	48	686-694	687.25	692.75	693.25	693.75
	49	694-702	695.25	700.75	701.25	701.75
	50	702-710	703.25	708.75	709.25	709.75

IRISH TV CHANNEL FREQUENCIES

STANDARD PAL I

Table D-7

BAND	CHANNEL #	BAND (MHz)	VISUAL (MHz)	AURAL (MHz)
IF	-	21.15-40.15	38.90(d)	32.90(e)
	1A	44.5-52.5	45.75	51.75
I	1B	52.5-60.5	53.75	59.75
	1C	60.5-68.5	61.75	67.75
	1D	174-182	175.25	181.25
	1E	182-190	183.25	189.25
III	1F	190-198	191.25	197.75
	1G	198-206	199.25	205.25
	1H	206-214	207.25	213.25
	1J	214-222	215.25	221.25

ITALIAN TV CHANNEL FREQUENCIES

STANDARD PAL B

Table D-8

BAND	CHANNEL #	BAND (MHz)	VISUAL (MHz)	AURAL (MHz)
IF	-	31.15-40.15	38.90	33.40
I	A	52.5-59.5	53.75	59.25
	B	61-68	62.25	67.75
II	C	81-88	82.25	87.75
	D	174-181	175.25	180.75
	E	182.5-189.5	183.75	189.25
	F	191-198	192.25	197.75
III	G	200-207	201.25	206.75
	H	209-216	210.25	215.75
	H1	216-223	217.25	222.75
	H2	223-230	224.25	229.75

JAPANESE TV CHANNEL FREQUENCIES

OFF-AIR AND CABLE

Table D-9

LOW-MID-HIGH BANDS

Ch. #	BW	VISUAL	AURAL	SAME AS US CH. #
IF	41.0-47.0	45.75	41.25	IF
J1	90-96	91.25	95.75	
J2	96-102	97.25	101.75	
J3	102-108	103.25	107.75	
JC13	108-114	109.25	113.75	A-2
JC14	114-120	115.25	119.75	A-1
JC15	120-126	121.25	125.75	A (14)
JC16	126-132	127.25	131.75	B (15)
JC17	132-138	133.25	137.75	C (16)
JC18	138-144	139.25	143.75	D (17)
JC19	144-150	145.25	149.75	E (18)
JC20	150-156	151.25	155.75	F (19)
JC21	156-162	157.25	161.75	G (20)
JC22	164-170	165.25	169.75	
J4	170-176	171.25	175.75	
J5	176-182	177.25	181.75	
J6	182-188	183.25	187.75	
J7	188-194	189.25	193.75	
J8	192-198	193.25	197.75	10
J9	198-204	199.25	203.75	11
J10	204-210	205.25	209.75	12
J11	210-216	211.25	215.75	13
J12	216-222	217.25	221.75	J

MOROCCAN TV CHANNEL FREQUENCIES

STANDARD PAL B

Table D-10

BAND	CHANNEL #	BAND (MHz)	VISUAL (MHz)	AURAL (MHz)
IF	-	33.15-40.15	38.90	33.40
III	M4	162-169	163.25	168.75
	M5	170-177	171.25	176.75
	M6	178-185	179.25	184.75
	M7	186-193	187.25	192.75
	M8	194-201	195.25	200.75
	M9	202-209	203.25	208.75
	M10	210-217	211.25	216.75

NEW ZEALAND UHF FREQUENCIES*

Table D-11

	Ch.	Lower	Visual	Color	Aural	Nicam	Upper
BAND IV	26	510	511.25	515.68	516.75	517.1	517.35
	27	518	519.25	523.68	524.75	525.1	525.35
	28	526	527.25	531.68	532.75	533.1	533.35
	29	534	535.25	539.68	540.75	541.1	541.35
BAND V	30	542	543.25	547.68	548.75	549.1	549.35
	31	550	551.25	555.68	556.75	557.1	557.35
	32	558	559.25	563.68	564.75	565.1	565.35
	33	566	567.25	571.68	572.75	573.1	573.35
	34	574	575.25	579.68	580.75	581.1	581.35
	35	582	583.25	587.68	588.75	589.1	589.35
	36	590	591.25	595.68	596.75	597.1	597.35
	37	598	599.25	603.68	604.75	605.1	605.35
	38	606	607.25	611.68	612.75	613.1	613.35
	39	614	615.25	619.68	620.75	621.1	621.35
	40	622	623.25	627.68	628.75	629.1	629.35
	41	630	631.25	635.68	636.75	637.1	637.35
	42	638	639.25	643.68	644.75	645.1	645.35
	43	646	647.25	651.68	652.75	653.1	653.35
	44	654	655.25	659.68	660.75	661.1	661.35
	45	662	663.25	667.68	668.75	669.1	669.35
	46	670	671.25	675.68	676.75	677.1	677.35
	47	678	679.25	683.68	684.75	685.1	685.35
	48	686	687.25	691.68	692.75	693.1	693.35
	49	694	695.25	699.68	700.75	701.1	701.35
	50	702	703.25	707.68	708.75	709.1	709.35
	51	710	711.25	715.68	716.75	717.1	717.35
	52	718	719.25	723.68	724.75	725.1	725.35
	53	726	727.25	731.68	732.75	733.1	733.35
	54	734	735.25	739.68	740.75	741.1	741.35
	55	742	743.25	747.68	748.75	749.1	749.35
	56	750	751.25	755.68	756.75	757.1	757.35
	57	758	759.25	763.68	764.75	765.1	765.35
	58	766	767.25	771.68	772.75	773.1	773.35
	59	774	775.25	779.68	780.75	781.1	781.35
	60	782	783.25	787.68	788.75	789.1	789.35
	61	790	791.25	795.68	796.75	797.1	797.35
	62	798	799.25	803.68	804.75	805.1	805.35

* UHF Transmission Systems

CCIR System G, PAL color. Standard European 8MHz channel spacing at UHF (470-806 MHz).

RUSSIAN VHF TV CHANNELS

STANDARD PAL D

Table D-12

NO.	CHANNEL	BANDWIDTH	CARRIER FREQUENCY	
			VISUAL	AURAL
1	1	48.5 - 56.5	49.75	56.25
2	2	58.0 - 66.0	59.25	65.75
3	3	76.0 - 84.0	77.25	83.75
4	4	84.0 - 92.0	85.25	91.75
5	5	92.0 - 100.0	93.25	99.75
6	CK-1	110.0 - 118.0	111.25	117.75
7	CK-2	118.0 - 126.0	119.25	125.75
8	CK-3	126.0 - 134.0	127.25	133.75
9	CK-4	134.0 - 142.0	135.25	141.75
10	CK-5	142.0 - 150.0	143.25	149.75
11	CK-6	150.0 - 158.0	151.25	157.75
12	CK-7	158.0 - 166.0	159.25	165.75
13	CK-8	166.0 - 174.0	167.25	173.25
14	6	174.0 - 182.0	175.25	181.75
15	7	182.0 - 190.0	183.25	189.75
16	8	190.0 - 198.0	191.25	197.75
17	9	198.0 - 206.0	199.25	205.75
18	10	206.0 - 214.0	207.25	213.75
19	11	214.0 - 222.0	215.25	221.75
20	12	222.0 - 230.0	223.25	229.75

SOUTH AFRICAN CHANNELS

PAL I

Table D-13

CHANNEL	BW(MHz)	VISUAL	AURAL
IF	37.15-40.15	38.90	32.90
4	174-182	175.25	181.25
5	182-190	183.25	189.25
6	190-198	191.25	197.25
7	198-206	199.25	205.25
8	206-214	207.25	213.25
9	214-222	215.25	221.25
10	222-230	223.25	229.25
11	230-238	231.25	237.25
13	246-254	247.43	253.25
21	470-478	471.25	477.25
22	478-486	479.25	485.25
23	486-494	487.25	493.25
24	494-502	495.25	501.25
25	502-510	503.25	509.25
26	510-518	511.25	517.25
27	518-526	519.25	525.25
28	526-534	527.25	533.25
29	534-542	535.25	541.25
30	542-550	543.25	549.25
31	550-558	551.25	557.25
32	558-566	559.25	565.25
33	566-574	567.25	573.25
34	574-582	575.25	581.25
35	582-590	583.25	589.25
36	590-598	591.25	597.25
37	598-606	599.25	605.25
39	614-622	615.25	621.25
40	622-630	623.25	629.25
41	630-638	631.25	637.25
42	638-646	639.25	645.25
43	646-654	647.25	653.25
44	654-662	655.25	661.25
45	662-670	663.25	669.25
46	670-678	671.25	677.25
47	678-686	679.25	685.25
48	686-694	687.25	693.25
49	694-702	695.25	701.25
50	702-710	703.25	709.25
51	710-718	711.25	717.25
52	718-726	719.25	725.25
53	726-734	727.25	733.25
54	734-742	735.25	741.25
55	742-750	743.25	749.25
56	750-758	751.25	757.25
57	758-766	759.25	765.25
58	766-774	767.25	773.25
59	774-782	775.25	781.25
60	782-790	783.25	789.25
61	790-798	791.25	797.25
62	798-806	799.25	805.25
63	806-814	807.25	813.25
64	814-822	815.25	821.25
65	822-830	823.25	829.25
66	830-838	831.25	837.25
67	838-846	839.25	845.25
68	846-854	847.25	853.25

WESTERN EUROPEAN CHANNELS

(Users include Scandinavia, Israel, South Africa)

Standard PAL B&G

Table D-14

TV Bands	Ch.	Channel frequency MHz	Visual carrier MHz	Aural carrier MHz
Standard B&G Europe				
I	2	47-54	48.25	53.75
	3	54-61	55.25	60.75
	4	61-68	62.25	67.75
Midband Channels	S 2	111-118	112.25	117.75
	S 3	118-125	119.25	124.75
	S 4	125-132	126.25	131.75
	S 5	132-139	133.25	138.75
	S 6	139-146	140.25	145.75
	S 7	146-153	147.25	152.75
	S 8	153-160	154.25	159.75
	S 9	160-167	161.25	166.75
	S10	167-174	168.25	173.75
III	5	174-181	175.25	180.75
	6	181-188	182.25	187.75
	7	188-195	189.25	194.75
	8	195-202	196.25	201.75
	9	202-209	203.25	208.75
	10	209-216	210.25	215.75
	11	216-223	217.25	222.75
	12	223-230	224.25	229.75
Superband Channels	S11	230-237	231.25	236.75
	S12	237-244	238.25	243.75
	S13	244-251	245.25	250.75
	S14	251-258	252.25	257.75
	S15	258-265	259.25	264.75
	S16	265-272	266.25	271.75
	S17	272-279	273.25	278.75
	S18	279-286	280.25	285.75
	S19	286-293	287.25	292.75
	S20	293-300	294.25	299.75
Extended Superband Channels	S21	302-310	303.25	308.75
	S22	310-318	311.25	316.75
	S23	318-326	319.25	324.75
	S24	326-334	327.25	332.75
	S25	334-342	335.25	340.75
	S26	342-350	343.25	348.75
	S27	350-358	351.25	356.75
	S28	358-366	359.25	364.75
	S29	366-374	367.25	372.75
	S30	374-382	375.25	380.75
	S31	382-390	383.25	388.75
	S32	390-398	391.25	396.75
	S33	398-406	399.25	404.75
	S34	406-414	407.25	412.75
	S35	414-422	415.25	420.75
	S36	422-430	423.25	428.75
	S37	430-438	431.25	436.75
	S38	438-446	439.25	444.75
IV	21	470-478	471.25	476.75
	22	478-486	479.25	484.75
	23	486-494	487.25	492.75
	24	494-502	495.25	500.75
	25	502-510	503.25	508.75
	26	510-518	511.25	516.75
	27	518-526	519.25	524.75
	28	526-534	527.25	532.75
IV	29	534-542	535.25	540.75
	30	542-550	543.25	548.75
	31	550-558	551.25	556.75
	32	558-566	559.25	564.75
	33	566-574	567.25	572.75
	34	574-582	575.25	580.75
	35	582-590	583.25	588.75
	36	590-598	591.25	596.75
	37	598-606	599.25	604.75
V	38	606-614	607.25	612.75
	39	614-622	615.25	620.75
	40	622-630	623.25	628.75
	41	630-638	631.25	636.75
	42	638-646	639.25	644.75
	43	646-654	647.25	652.75
	44	654-662	655.25	660.75
	45	662-670	663.25	668.75
	46	670-678	671.25	676.75
	47	678-686	679.25	684.75
	48	686-694	687.25	692.75
	49	694-702	695.25	700.75
	50	702-710	703.25	708.75
	51	710-718	711.25	716.75
	52	718-726	719.25	724.75
	53	726-734	727.25	732.75
	54	734-742	735.25	740.75
	55	742-750	743.25	748.75
	56	750-758	751.25	756.75
	57	758-766	759.25	764.75
	58	766-774	767.25	772.75
	59	774-782	775.25	780.75
	60	782-790	783.25	788.75
	61	790-798	791.25	796.75
	62	798-806	799.25	804.75
	63	806-814	807.25	812.75
	64	814-822	815.25	820.75
	65	822-830	823.25	828.75
	66	830-838	831.25	836.75
	67	838-846	839.25	844.75
	68	846-854	847.25	852.75
	69	854-862	855.25	860.75

Extended Superband Channels			Visual carrier MHz
	S21	302-314	303.25
	S22	314-326	315.25
	S23	326-338	327.25
	S24	338-350	339.25
	S25	350-362	351.25
	S26	362-374	363.25
	S27	374-386	375.25
	S28	386-398	387.25
	S29	398-410	399.25
	S30	410-422	411.25
	S31	422-434	423.25
	S32	434-446	435.25

Appendix E
Service & Product Suppliers*

Addressable Taps

American Lightwave Systems
999 Research Parkway
Meriden, CT 06450
Phone: 203-265-8802
Fax: 203-265-8746

Blonder-Tongue Laboratories
Old Jack Brown Road
Old Bridge, NJ 08857
Phone: 908-679-4000
Fax: 908-679-4353

Viewsonics
6454 West Rogers Circle
Boca Raton, FL 33487
Phone: 800-654-7600
Fax: 561-998-9594

Auditors

Action Plus Marketing Inc.
5807 East Skelly Drive Suite 400
Tulsa, OK 74135
Phone: 800-256-0330
Fax: 918-627-2692

BCI Inc.
5160 Parkstone Drive
Chantilly, VA 22021-3813
Phone: 703-222-8300
Fax: 703-222-0205

Cable Management Services
4059 River Road
Schenectady, NY 12309-1518
Phone: 518-785-9325
Fax: 518-785-9325

Contract Installers Inc.
P.O. Box 1564
Appleton, WI 54986-1564
Phone: 414-582-7087
Fax: 414-582-7528

Pinnacle Cable Services
Five Greentree Centre Suite 313
Marlton, NJ 08053
Phone: 609-983-8330
Fax: 609-983-8255

Rent-A-Tech
4987 Tenterden Drive
Syracuse, N.Y. 13215
Phone: 315-463-7656
Fax: 315-463-7681

RCH Cable
301 Route 130
Cinnaminson, NJ 08077
Phone: 609-786-1701
Fax: 609-786-0121

RMS
P.O. Box 110245
Carrollton TX 75011-0245
Phone: 800-552-0204
Fax: 972-713-0719

SRS Communications Corporation
80 Vanderbuilt Avenue
West Hartford, CT 06110
Phone: 860-953-3770
Fax: 860-953-3772

Computer Software

Anderson-Bell Corporation
P.O. Box 5160
Arvada, CO 80005
Phone: 800-745-9751
Fax: 303-940-0595

Backdoor Group Inc.
10500 North Port Washington Road
#107
Meguan, WI 53092
Phone: 414-241-3037
Fax: 414-241-3125

Lotus Development Corporation
55 Cambridge Parkway
Cambridge, MA 02142
Phone: 800-343-5414
Fax: 617-693-3899

Converters & Scramblers

Cabletenna
440 Forsgate Drive
Cranbury, NJ 08512
Phone: 609-395-9400
Fax: 609-395-1927

For-A Corporation of America
11095 Knott Avenue
Cypress, CA 90630
Phone: 714-894-3311
Fax: 714-894-5399

* Many of the suppliers listed above make or distribute equipment in a variety of different categories. They have been listed by their major activity. Check with the respective supplier for products in other categories.

Decoders

Leitch Inc.
920 Corporate Lane
Chesapeake, VA 23220
Phone: 800-231-9673
Fax: 757-548-4210

Microdyne Corporation
3601 Eisenhower Avenue
Alexandria, VA 22304
Phone: 703-739-0500
Fax: 703-329-3722

Monroe Electronics
100 Housel Avenue
Lyndonville, NY
Phone: 800-821-6001
Fax: 716-765-9330

Magazines & Publishers

Baylin Publications
1905 Mariposa
Boulder, CO
Phone: 303-449-4551
Fax: 303-939-8720

Communications Engineering Design
P.O. Box 10728
Riverton, NJ 08076-0728
Phone: 609-786-0501
Fax: 212-887-8493

Communications Technology
1201 Seven Locks Road
Rockville, MD 20854
Phone: 301-340-1520
Fax: 301-340-0542

Electric Press
7399 Taft Park Drive
East Syracuse, NY 13057
Phone: 315-452-5488
Fax: 315-452-5850

Independent Cable News
5931 South Middlefield Road
Suite 102
Littleton, CO 80123
Phone: 303-797-8522
Fax: 303-797-8708

International Cable
1201 Seven Locks Road
Rockville, MD 20854
Phone: 301-340-1520
Fax: 301-340-0542

Multichannel News
825 Seventh Avenue
New York, NY 10019
Phone: 212-887-8400
Fax: 212-887-8384

Private Cable Update
4451 I-70 Drive N.W.
Columbia, MO 65202
Phone: 800-445-6164
Fax: 573-445-0757

Private Cable & Wireless Cable
10500 Richmond Avenue Suite 275
Houston, TX 77042
Phone: 713-975-0030
Fax: 713-974-0909

Searle Publishing Company
2329 West Main Street
Littleton, CO 80120
Phone: 303-797-8522
Fax: 303-797-8708

Television & Cable Factbook
Warren Publishing
2115 Ward Court, NW
Washington, D.C. 20037
Phone: 202-872-9200
Fax: 202-293-3435

Lock Manufacturers

EEG Enterprises Inc.
1 Rome Street
Farmingdale, NY 11735
Phone: 516-293-7472
Fax: 516-293-7417

Multilink
587 Ternes Avenue
Elyria, OH 44035
Phone: 216-366-6966
Fax: 216-366-6802

Locking Enclosures

Power & Telephone Supply Co.
2673 Yale Avenue
Memphis, TN 38112
Phone: 800-238-7514
Fax: 901-320-3082

Reltec
21133 Addison Street
Franklin Park, IL 60131
Phone: 800-338-1951
Fax: 847-451-5629

Network Manufacturers

General Instrument Corporation
2200 Byberry Road
Hatsboro, PA 19040
Phone: 215-674-4800
Fax: 215-956-6494

Philips Broadband Networks
100 Fairgrounds Drive
Manlius, NY 13104
Phone: 800-448-5171
Fax: 315-682-9006

Scientific Atlanta
3845 Pleasantdale Road
Atlanta, GA 30340
Phone: 404-903-2530
Fax: 404-903-2591

Zenith Electronics Corporation
100 Milwaukee Avenue
Glenview, IL 60025
Phone: 847-391-7000
Fax: 847-391-7253

Regulatory Agencies

Federal Communications Commission
Cable Services Bureau
2033 M Street West
Washington, D.C. 20554
Phone: 202-418-7200

Tap Identification

Cabletek Center Products
1150 Taylor Street
Elyra, OH 44035
Phone: 216-365-3889
Fax: 216-322-0321

Diamond Communications Products
500 North Avenue
Garwood, NJ 07027
Phone: 908-789-1400
Fax: 908-789-7975

Telecrafter
12687 West Cedar Drive
Lakewood, CO 80228
Phone: 800-257-2448
Fax: 303-986-1042

Tap Locks

Cable-Lock Connectors
358 Humberline Drive
Etubicoke, ON M9W 5S3
Canada
Phone: 416-798-8558
Fax: 416-798-8563

Trade Associations

National Cable Television Association
1724 Massachusetts Avenue N.W.
Washington, D.C. 20036
Phone: 202-775-3550
Fax: 202-775-3604

Small Cable Business Association
7901 Stoneeridge Drive
Suite 404
Pleasanton, CA 94588
Phone: 510-463-0404
Fax: 510-463-9627

Society of Cable Television Engineers
140 Philips Road
Exton, PA 19341
Phone: 610-363-6888
Fax: 610-363-5898

Trap Manufacturers

Arcom Laboratories
185 Ainsley Drive
Syracuse, NY 13210
Phone: 800-448-1655
Fax: 315-422-2963

C&E Corporation
7397 Taft Park Drive
East Syracuse, NY 13057
Phone: 800-882-1587
Fax: 315-452-0732

Eagle Comtronics
4562 Waterhouse Road
Clay, NY 13041
Phone: 315-622-3402
Fax: 315-622-3800

Gamco
45A Walnut Avenue
Clark, NJ 07066
Phone: 908-381-0700
Fax: 908-381-6168

Pico Products
12500 Foothill Blvd.
Lakeview Terrance, CA 91342
Phone: 818-897-0028
Fax: 818-899-1165

Product Production Company
One Mezzy Lane
Box 280
Manlius, NY 13104
Phone: 315-431-7200
Fax: 315-431-7201

Vehicle Equipment

American Van Equipment
1985 Rutgers University Blvd.
Lakewood, NJ 08701
Phone: 800-526-4743
Fax: 800-833-8266

Masterack
905 Memorial Drive, S.E.
Atlanta, GA 30348
Phone: 404-522-8368
Fax: 404-659-9316

Appendix F
CATV Distributors

AUSTRALIA

AV COMM PTY LTD
PO BOX 225, BALGOWLAH 2093, 198 CONDAMINI STREET
BALGOWLAH, AUSTRALIA
TEL: 61-2-949-7417
FAX: 61-2-949-7095

BELGIUM

SKYLINE COMMUNICATIONS
ROESELAARSESTRAAT 648
B-8870 IZEGEM, BELGIUM
TEL: 32051-313569
FAX: 32051-310129

CANADA

INCOSPEC, INC.
3150 DELAUNAY
LAVAL, H7L 5E1, QUEBEC CANADA
TEL: 514-686-0033
FAX: 514-688-7709

TEL-VISION
4100 CHEMIN CHAMBLY STREET
HUBERT, J3Y 3M3, QUEBEC CANADA
TEL: 514-676-7076
FAX: 514-676-5960

ENGLAND

ALBAN ELECTRONICS LTD
6 CAXTON CENTRE
PORTERS WOOD, ST. ALBANS, HERTS AL4 6SF
TEL: 727-83-2266
FAX: 44-1727-810-546

BENTLEY WALKER LTD.
116 ELM GROVE, HAYLING ISLAND
HAMPSHIRE PO119E, ENGLAND
TEL: 44-705-463943
FAX: 44-705-461465

FRANCE

JP2SA/TEXSCAN
15, RUE CORBUSIER
94035 CRETIEL, FRANCE
TEL: 331-439-94732
FAX: 331-439-90758

ISRAEL

ROTAL TELECOMM & RECEIVING SYSTEMS
3 EFAL STREET, PO BOX 3779, PETACH
TIKVA 49130, ISRAEL
TEL: 972-3-922-8040
FAX: 972-3-922-3299

JAPAN

UNI COMM TRADING
SHITE 5 KUMI
OITA CITY 870, JAPAN
TEL: 0975-44-1552
FAX: 0975-43-1116

PHILIPPINES

WAVELINK COMMUNICATIONS & SATELLITE PHILS.
UNIT 1535, GUADALUPE BLISS
MAKATI CITY, PHILIPPINES
TEL: 632-433-9737
FAX: 632-924-9403

NEW ZEALAND

FAR NORTH CABLE TV
PO BOX 330, MANGONUI
FAR NORTH, NEW ZEALAND
TEL: 64-9-406-0651
FAX: 64-9-406-1083

TELEQUIPMENT PACIFIC LTD.
LEVEL 2, 195 VICTORIA STREET
P.O. BOX 11-169
WELLINGTON, NEW ZEALAND
TEL: 64-4-384-1927
FAX: 64-4-385-9892

SOUTH AFRICA

TELEMEDIA PTY LTD
PO BOX 783515
SANDTON, SOUTH AFRICA
TEL: 803-3353/4
FAX: 803-25343

SPAIN

VANDETEL
C/.ANTONIO MILLON 6-EDIF VENUS 30B
NERJA 29780, MALAG, SPAIN
TEL: 95252-5327
FAX: 95252-3072

SWEDEN

WAVELINE COMM AB
VIPEVAGEN 6, S-21611
MALMO, SWEDEN
TEL: 46-40-164-266
FAX: 46-40-150-507

SPECIAL ELEKTRONIK
BOX 8065
S-650 08 KARLSTAD, SWEDEN
TEL: 054-53-4980
FAX: 054-53-4988

SWITZERLAND

REDIFFUSION AG
ZOLLSTRASSE 42
CH-8021 ZURICH, SWITZERLAND
TEL: 277 91 11
FAX: 272 81 84

TAIWAN

FAR REACHING TRADE ASSOCIATED INC.
1F, NO 15-2 LANE 141 CHUNG SHAN NORTH ROAD SEC 7
TAIPEI ROC, TAIWAN
TEL: 886-2-8201-067
FAX: 886-2-820-2417

SPECTRUM
4F 50 SUNG CHIANG ROAD
TAIPEI, TAIWAN
TEL: 886-2-511-0427
FAX: 886-2-561-0453

THAILAND

AEROCOMM SATELLITE TECHNOLOGY COMPANY LTD.
89 & 89/1 INTAMARA 41, KWAND DINGAENG
BANGKOK 10320, THAILAND
TEL: 662-693-8300
FAX: 662-693-8304

USA

ACS ENTERPRISES
2510 METROPOLITAN DRIVE
FEASTERVILLE-TREV, PA 19053-6738
TEL: 215-396-9400
FAX: 215-396-9550

ATV RESEARCH
PO BOX 620
DAKOTA CITY, NE 68731
TEL: 402-987-3771
FAX: 402-987-3709

CABLE TECHNOLOGY ASSOCIATES
160 DWIGHT PARK CIRCLE, STE. 1
SYRACUSE, NY 01085
TEL: 315-451-9450
FAX: 315-451-9453

CABLE TRONIC SYSTEMS
756 CRESTVIEW ROAD
VISTA, CA 92083
TEL: 619-726-1706

CAMCO CABLE SERVICES
3958 NW 167TH STREET
MIAMI, FL 33054
TEL: 305-621-0090
FAX: 305-621-8651

D. CO MARKETING
27401 LOS ALTOS, STE. 270
MISSION VIEJO, CA 92691
TEL: 714-367-1700
FAX: 714-367-1734

D.F. COUNTRYMAN COMPANY
480 NORTH PRIOR AVENUE
ST. PAUL, MN 55104
TEL: 612-645-9154
FAX: 612-645-1298

DAWN SATELLITE
PO BOX 9
LAKE ORION, MI 48359
TEL: 810-391-9200
FAX: 810-969-0377

MARSHALL INDUSTRIES, INC.
614 EAST 3900 SOUTH
SALT LAKE CITY, UT 84107
TEL: 801-266-2428
FAX: 801-268-92455

MEGA HERTZ CORPORATION
6940 S. HOLLY CIRCLE, STE. 200
ENGLEWOOD, CO 80112
TEL: 303-779-1717
FAX: 303-779-1749

NORTH AMERICAN CABLE EQUIPMENT CO
893 SOUTH MATLACK STREET, STE. 170
WESTCHESTER, PA 19382
TEL: 610-429-1821
FAX: 610-429-3060

PASSIVE DEVICES
6353 WEST ROGERS CIRCLE, BAY 6
BOCA RATON, FL 33487
TEL: 800-242-1606
FAX: 516-998-0608

PENSACOLA ELECTRONICS
PO BOX 18810
PENSACOLA, FL 32505
TEL: 904-478-3771
FAX: 904-479-1455

PHOENIX TELETRONICS
26027 HUNTINGTON LANE, STE. D
VALENCIA, CA 91355-1145
TEL: 805-294-1810
FAX: 805-294-1820

QINTAR, INC.
700 JEFFERSON AVENUE
ASHLAND, OR 33009
TEL: 541-488-5500
FAX: 541-488-5567

SPECTRUM
3371 BROWEN AVENUE
MOUNTAINVIEW, CA 94040
TEL: 415-961-6099
FAX: 415-988-8858

SPECTRUM
1791 HURSTVIEW DRIVE
HURST, TX 76054
TEL: 800-628-0088
FAX: 817-280-0745

TONER CABLE
969 HORSAM ROAD
HORSHAM, PA 19044
TEL: 215-675-2053
FAX: 215-675-7543

VIEWSONICS
6454 WEST ROGERS CIRCLE
BOCA RATON, FL 33487
TEL: 800-645-7600
FAX: 516-998-9594

TECHNICAL GLOSSARY

A

A/B Switch: A two position coaxial switch for routing either of two radio frequency inputs (A or B) to a single output while providing high isolation between the two inputs. Can also be used to route a common input to either of two outputs (A or B).

Absorber: See: "Microwave Absorber."

AC (Alternating Current): See: "Alternating Current."

A/D (Analog to Digital) Converter: See: Analog to Digital Converter.

Addressable Converter Box: A subscriber converter box with a unique name, address, or designation which allows a central processor to send instructions to only that converter box.

Addressable Tap: An addressable security device used for limiting the signals on a subscriber's drop line to only those channels which the subscriber is authorized to receive.

Ad Insertion Equipment: Tape or solid state equipment for interrupting programming on a specific channel and putting prerecorded advertising on the channel.

Adjacent Channel: A channel directly above or directly below a specific channel.

AF (Audio Frequency): See: "Audio Frequency."

AFC (Automatic Frequency Control): See: "Automatic Frequency Control."

A Group: See: "Group A."

AGC (Automatic Gain Control): See: Automatic Gain Control.

Air Coax: A form of coaxial cable which uses air as a dielectric.

Air Shrink Boot: A plastic sleeve for weatherproofing connections which shrinks when heated with hot air.

ALC (Automatic Level Control): See: "Automatic Gain Control."

Algorithm: A set of instructions or computational process for producing some desired result.

Alternating Current (AC): A current which flows first in one direction and then in another direction. Technically there are many kinds of AC at audio frequencies, radio frequencies and at power supply frequencies. Often in the United States the term AC is used to mean standard AC Power at 60 Hz.

AM (Amplitude Modulation): See: "Amplitude Modulation."

AM Detector: An electrical circuit which frequently uses diodes and filtering circuits to remove amplitude modulation from another radio frequency carrier or wave form.

American Standard Code II (ASCII): A more or less universal seven bit computer code for transferring data between computers in the United States.

AML (Amplitude Modulated Link): See: "Amplitude Modulated Link."

Ampere: A unit for measuring current flow. See: "Current."

Amplifier: A device which turns a relative small signal into a relatively large signal. There are three types: voltage amplifiers, current amplifiers, and power amplifiers.

Amplitude: The extreme range or magnitude of a waveform usually represented along the y-axis of a graph.

Amplitude Equalizer: A device which corrects for differences in carrier levels caused by propagation anomalies.

Amplitude Modulation (AM): A form of modulation which uses the level of a signal to carry another signal.

Amplitude Modulated Link (AML): An amplitude modulated microwave link usually used for transporting programs over long distances from one location to another. AMLs are sometimes used to import out-of-town television stations.

Analog: Processing a signal as a continuous wave form as distinct from digital encoding. Analog signals may be amplitude, frequency, or phase modulated.

Analog Channel Compression: A technique for squeezing more than one program into a single channel using analog processes.

Analog Inverter: A device which inverts a wave form.

Analog-to-Digital (A/D) Converter: A device for translating or encoding an analog wave form into digital code.

AND Gate: A digital device which outputs a high state if either of its inputs are high.

Antenna: A device for transmitting (radiating) or receiving radio frequency energy.

Antenna Coupling: Electro-magnetic interaction between two antennas in close proximity with each other. Such antennas can act as parasitic elements with respect to each other changing the patterns of the antennas.

Antenna Efficiency: Refers to the degree to which an antennas power is radiated in relation to the power which is wasted in various losses.

Antenna Feed: An antenna device which collects radio signals from space and puts them onto a coaxial line. See: "Feedhorn."

Antenna Gain: The measure of an antenna radiation or reception pattern in relation to either an isotopic antenna or some other antenna pattern.

Antenna Illumination: The degree to which the radiation pattern of an antenna feed pattern covers an antenna reflector.

Antenna Power Gain: An FCC term for the square root of the ratio of the root-mean-square free space field intensity produced at one mile in a horizontal plane in micro-volts per meter for one kilowatt antenna input power (137.6 mV/m). This ratio may be expressed in dB.

Antenna Power Input: An FCC term for the RF peak or RMS power supplied to the antenna from its associated transmission line and matching network.

Antenna Shroud: A cylindrical hood which fits over the face of a parabolic dish with microwave absorbent material on the inside for reducing antenna side lobes.

Antenna Structure: An FCC term which refers to the whole tower system including the radiation system, supporting structure and any surmounted appurtenances.

Aperture: An opening for signals or light to pass through in an antenna feed or some other device.

ASC (Automatic Slope Control): See: "Automatic Slope Control."

Astable (Free Running) Multivibrator: A free running multivibrator which oscillates or changes back and forth between two states. Frequently used for timing.

ACSII (American Standard Code II): See: "American Standard Code II."

Assigned Frequency: The frequency listed for a broadcast station in its FCC license or instrument of authorization.

Atta-: A metric prefix which means 1/1,000,000,000,000,000,000 or 10^{-18}.

Attenuation: The reduction in the amplitude of a signal (often expressed in decibels) resulting from an impedance loss as it travels through some medium.

Attenuator: A passive device for reducing the amplitude of a wave form without distortion. Attenuation levels are usually expressed in ohms (impedance) or decibels (signal reduction levels).

Audio: Frequencies within the range of human hearing usually between 30 Hz and 20 KHz.

Audio Frequency (AF): See: "Audio."

Audio Modulator: A device which combines audio with higher frequency radio signals for transmission.

Automatic Back-Up System: Usually a switching network designed to automatically take a malfunctioning transmitter off line and re-route programming to a back-up transmitter.

Automatic Fine Tuning (AFT): An equipment feature which automatically corrects frequency drift.

Automatic Frequency Control (AFC): An equipment feature which automatically locks onto a specific frequency to prevent frequency drift.

Automatic Gain Control (AGC): An equipment feature that automatically maintains an output level for varying input levels.

Automatic Level Control (ALC): See: "Automatic Gain Control."

Automatic Slope Control (ASC): A device which automatically changes the slope of an amplifier's curve to compensate for temperature changes.

Automatic Volume Control (AVC): See: "Automatic Gain Control."

AVC (Automatic Volume Control): See: "Automatic Gain Control."

Azimuth: An angular measure in degrees around the horizon.

Azimuth Beam Width: The angular measure of an antenna pattern as viewed along the horizon. It is sometimes called the horizontal beam width.

B

Bandpass Filter (BPF): A device which passes a specific range of frequencies and (in theory) blocks all others.

Band Separator: See: "Frequency Splitter."

Bandstop Filter (BSF): A device which blocks a specific range of frequencies and (in theory) passes all others.

Band Width: A specific range of frequencies defined by an upper and lower limit. Frequently the - 3 dB points of a pass band are used to define band limits. For communications purposes the FCC defines the bandwidth of specific channels.

Base Band Audio: The range of frequencies from 0 to 20 KHz.

Base Band Video: The band of frequencies from 0 to 4.2 MHz.

Baud: The reciprocal of time for the shortest pulse or signal element transmitted.

Baudot Code: A five bit teletype code used for representing the alphabet.

Baud Rate: The maximum rate or speed at which a system can transmit or receive pulses.

Balun: An impedance matching transformer. Baluns are frequently used for matching a television antennas to coaxial lines although there are numerous other applications. See: "Impedance Matching Network."

Beacon: A flashing warning light mounted on top of a tower.

Beam Bender: A name used for wireless relays. See: "Signal Booster" and "Beambender©."

Beambender©: A copyright term or trade name belonging to *California Amplifier* for their wireless relay kit.

Beam Tilt: See: "Down Tilt."

Beam Width: The width of the main lobe of an antenna pattern. Usually the beam width of an antenna's main lobe is defined as 3 dB down from the peak of the lobe. Beam width may be measured either vertically or horizontally. See: "Azimuth Beamwidth" and "Elevation Beamwidth."

Beat: A sum or difference frequency resulting from the mixing of two signals. See: "Heterodyne."

B Group: See: "Group B."

Binary: A two symbol number system used in digital computers which utilizes only the symbols zero and one.

Bipod: An antenna mounting system which has two supporting legs.

Bistable Multivibrator (Flip Flop): A multivibrator with two stable states which changes states when triggered. See: "Flip Flop."

Bit: A binary digit consisting of either a high or low state which may be represented as a zero (0) or one (1).

Block Down Converter: A device which lowers a whole band of frequencies from one band to another lower band.

BMC (Business Management Computer): See: "Business Management Computer."

BNC Connector: A coaxial connector which uses a twist lock device to hold it on.

Boolean Algebra: A system of symbolic logic first developed by George Boole during the 19th Century and subsequently adopted for digital computer systems. While Boolean Algebra essentially follows the same rules of logic as other systems developed by the ancient Greeks, it is a more appropriate system for circuits. Boole's actual notation was different from that used today.

Bow-Tie Reflector: A small reflector antenna frequently used at UHF and microwave frequencies with a feed which looks like a bow-tie.

BPF (Bandpass Filter): See: "Bandpass Filter."

Braid: Inter-woven wire used either as ground wire or as a coaxial cable shield.

Bridger Amplifier: A CATV amplifier similar to a trunk amplifier with a power divider for placing signals on several feeder lines. Bridgers are usually used on truck lines.

Broadband Amplifier: An amplifier with a relatively wide frequency response as distinguished from a single channel or narrower band amplifier.

Broadband Gateway™: A device developed by *Philips Broadband* for interfacing a subscriber's telephone, broadband computer modem, and television with a CATV network.

BSF (Bandstop Filter): See: "Bandstop Filter."

Buffer: An amplifier used to isolate two other amplifier stages from each other.

Bulkhead: See: "Ground Bulkhead."

Business Management Computer (BMC): The computer system used at a CATV or MMDS business office to keep track of subscriber accounts.

Byte: a group of eight bits.

C

C/I (Carrier-to-Interference Ratio): See: "Carrier-to-Interference Ratio" and "Desired-to-Undesired Carrier Ratio."

C/N (Carrier-to-Noise Ratio): See: "Carrier-to-Noise Ratio."

Cable: Usually a coaxial cable but can sometimes mean a large wire cable. See: "Coaxial cable."

Capacitance: A property of capacitors (measured in farads) which tends to oppose any change in current

flow. This property stems from energy in the electrostatic field between two separate electrodes or plates.

Capacitive Reactance: Capacitive opposition to any change in current flow measured in ohms.

C-Band: A band of frequencies between 3.7 and 4.2 GHz used for satellite relay broadcasting to TVRO earth stations.

CCTV (Closed Circuit Television): See: "Closed Circuit Television."

Cable: A wire. Usually the term cable refers to coaxial cable or a cable television system.

Cable Loss: The insertion loss of a coaxial cable or wire.

Cardioid Pattern: An antenna pattern similar to a half-hemisphere or heart shape.

Carrier: A radio frequency signal which is often modulated by a lower frequency signal carrying some form of intelligence for radio transmission.

Carrier-to-Interference (C/I) Ratio: The ratio of the amplitude of a radio frequency carrier to the amplitude of any other form of interference including both noise and other undesired carriers. The C/I is a broader measure than C/N because it include undesired radio frequency carriers. See: "Carrier-to-Interference Ratio."

Carrier-to-Noise (C/N) Ratio: The ratio of the amplitude of a radio frequency carrier to the amplitude of background noise.

CATV (Community Antenna Television): See: "Community Antenna Television."

Center Frequency: The unmodulated frequency of an FM or AM carrier.

Centi- : A metric prefix meaning one hundredth or 1/100 or 10^{-2}.

CFR (Code of Federal Regulations): See: "Code of Federal Regulations."

C Group: See: "Group C."

Channel: A defined bandwidth used for one communications link. In the US the FCC defines channel center frequencies and bandwidths.

Channel Compression: The process of fitting more than one program into a single channel. See: "Analog Channel Compression" and "Digital Channel Compression."

Channel Converter: A device which converts signals from one channel to another channel. There are two types - heterodyne converters and those which utilize frequency multiplication principles. See: "Heterodyne Converter" and "Processor."

Channel Processor: See: "Processor."

Channel Transmitter: See: "Single Channel Transmitter."

Channel Mapping: The dynamic process of broadcasting specific programs on various MMDS and ITFS channels according to a predetermined schedule with encoded data which re-routes the program to the same subscriber television channel regardless of MMDS/ITFS channel it was broadcast on.

Chimney Mount: A mounting system used for attaching an antenna mast to a brick chimney.

Cipher: A cryptological process for concealing some form of communicated intelligence utilizing a key or some algorithm. In a cipher elements of the communicated intelligence are rearranged and represented according to a process determined by the key. Technically there is a difference between codes and ciphers. Cipher processes are generally dynamic as distinct from static.

Circulator: A device used for isolating amplifier stages from each other or from other devices.

Clark Belt: A circular equatorial orbital path named after science fiction writer Arthur C. Clark. See: "Geosynchronous Orbit."

Class A Amplifier: An amplifier biased so that current flows throughout the entire signal cycle.

Class A-B Amplifier: An amplifier biased between Class A and Class B so that current flows for more than fifty percent of any signal cycle.

Class B Amplifier: An amplifier biased so that current flows current flows only during half of the signal cycle.

Class C Amplifier: An amplifier biased way beyond cut-off so that current flows only during a portion of the signal peaks. Use of class C amplifiers is frequently limited to only RF amplifiers using resonate tank circuits to complete the remainder of the signal cycle.

Clock Pulses: Timing Pulses. See: "Timing."

Closed Circuit Television (CCTV): An internal or private video circuit.

Coaxial Cable: A wire surrounded by another tubular conductor with an insulator between the inner wire and the outer tubular conductor. The term coaxial comes from the fact that both the inner and the outer conductors share the same axis.

Coaxial Lightning Arrester: See: "Coaxial Lightning Suppressor."

Coaxial Lightning Suppressor: A device which grounds a coaxial cable shield and shorts surge voltages on the inner conductor to ground.

Coaxial Switch: A switch used for disconnecting or re-routing signals on coaxial cables. See: "Transfer Switches."

Co-Channel: Same channel.

Co-Channel Interference: A form of in-channel interference from another station operating on the same channel or channels as the station experiencing interference.

Code: The process of representing some form of communicated intelligence. Most codes use substitution either for the purpose of security or for the purpose of processing information efficiently. Technically there is a difference between a code and cipher. Codes are usually static rather than dynamic.

Code of Federal Regulations (CFR): The official government publication containing FCC Rules & Regulations.

Coherent Interference: Any form of interference which is intelligible as a television picture. Typically either an off-set ghost of a strong television picture or a ghost of a completely different picture mixed with a strong picture. See: Non-Coherent Interference.

Combination Network: A network designed to combine two or more input channels into one output band with high isolation between the input channels. See: "Combiner."

Combiner: A network for putting two or more frequency bands or channels together for transmission along a single line.

Commercial Television (CTV): Television which is supported by commercial advertisers.

Common Mode Interference: Unwanted signals or interference which are common to both the input and output grounds and which are in-phase at both the input and the output. See: Differential Mode Interference.

Community Antenna Television (CATV): A cable television system.

Compass: A device for finding magnetic north or measuring magnetic azimuth.

Composite Triple Beat: Intermodulation involving three carriers beating together which results in horizontal streaking in television pictures. See: "Triple Beat."

Computer Generated Interference Analysis: A computer generated simulation (based upon information drawn from an FCC database) intended to determine whether adjacent transmitters will interfere with a transmitter or receiver located at a specific set

of coordinates. Also, a computer simulation intended to determine whether a transmitter will interfere with receivers in adjacent systems protected areas.

Connector: A device for connecting wires or cables to equipment or to other wires and cable. See: "F Connector," "N Connector," "SMA Connector," and "Waveguide Flange."

Converter: See: "Down-Converter;" "Up-converter;" "Set-Top Converter;" "Channel Converter and Block-Down Converter."

Corner Reflector: A broadband yagi like antenna frequently used in the UHF band with a V shaped reflector. MMDS corner reflectors are also made.

Counter: See: "Digital Counter."

CPR-340: Waveguide flange for WR-340.

CPR-430: Waveguide flange for WR-430.

Cross Modulation: The unintentional modulation of one radio frequency carrier by another carrier.

Cross Polarization: Polarization half way between the horizontal polarization and vertical polarization in order to receive signals polarized both ways at equal levels.

Cross Talk: Cross modulation between two adjacent channels. The term is usually used with audio.

CTV (Commercial Television): See: "Commercial Television."

Cut and Invert: An analog method of scrambling video involving the inversion of certain video lines.

Cut and Rotate: An analog technique for scrambling video involving the transposition of video lines.

Current: Electron flow through a conductor measured in amperes.

Cycle: One complete wave form which repeats itself.

D

D/A (Digital-to-Analog) Converter: See: "Digital-to-Analog Converter."

D/U (Desired-to-Undesired): See: "Desired-to-Undesired Interference Ratio."

Data Encryption Standard (DES): An encryption algorithm released by the Bureau of Standards for the protection of computer data.

dB (Decibel): See: "Decibel."

dBd: A decibel measure of gain or loss referenced to the gain of a dipole antenna.

dBi: A decibel measure of gain or loss measured in relation to an isotopic antenna pattern.

dBm: A decibel measure referenced to one milliwatt without reference to any impedance.

dBmV: A decibel measure in relation to one millivolt across a specific impedance. In CATV the impedance used is 75 ohms .

DBS (Direct Broadcast Satellite): A transmission system which allows subscribers to receive television directly from satellite relays in orbit around the earth.

dBW: A decibel measure referenced to one watt without reference to any impedance.

DC (Direct Current): See: "Direct Current."

DC Block: A device which blocks direct current but passes radio frequencies, audio frequencies, or alternating current depending upon the function of the block.

De-emphasis: The reverse of pre-emphasis. A process used in frequency modulated detectors to reverse pre-emphasis during transmission. See: "Pre-emphasis."

Deca-: A metric prefix meaning ten. Thus the word decade.

Deci-: A metric prefix meaning one tenth or 1/10 or

10^{-1}.

Decibel (dB): A logarithmic ratio comparing two voltages, currents, or power levels (usually input and output). One decibel represents one tenth of a Bel (the logarithmic ratio). A +3 dB gain represents a doubling of power while a -3 dB loss represents half of the power.

Decimal: An array of integers (0- 9) used to represent a fraction.

Decipher: Use of a cryptological process involving a key to recover information which has been enciphered. See: "Cipher."

Declination: See: "Declination Diagram."

Declination Diagram: A diagram on a topographical map which Shows the angular relation between true north, grid North, and magnetic north for a specific map sectional.

Decode: The process of recovering information which has been encoded. See: Code. Sometimes scrambling and security trapping techniques are called decoding.

Decoding: See: "Decode."

Decrypt: See: "Decipher."

Decryption: "Decipher."

Demodulator: A device used for removing signals from a carrier through the process of down conversion and detection.

DES (Data Encryption Standard): See: "Data Encryption Standard."

Desired-to-Undesired (D/U) Interference Ratio: The ratio of a desired RF carrier to an undesired RF carrier. This is a more narrow measure than the C/I ratio or the C/N ratio since it measures levels in relation to only undesired RF carriers. See: "Carrier-to-Interference Ratio" and "Carrier-to-Noise Ratio."

Descrambling: The reverse of scrambling. See: "Scrambling."

Detector: A device used to remove modulation from a radio frequency carrier or another wave form. There are generally two types of detectors: AM and FM. See: "AM Detector," "Ratio Detector," and "Discriminator."

D Group: See: "Group D."

Differential Mode Interference: Interference on a signal line (between ground and an input). Differential mode interference enters a receiver through the antenna. See: "Common Mode Interference."

Diffraction: See: "Microwave Diffraction."

Digital: A process of representing signals in terms of discrete high and low states.Use of pulsed codes.

Digital Channel Compression: The process of fitting more than one program into a single channel using digital techniques to eliminate redundant information.

Digital Counter: A digital or binary register for counting up or down.

Digital Inverter: A device which outputs a high state when its input is low or outputs a low state if its input is high.

Digital Modulation: An FCC term for the process by which some characteristic (frequency, phase, amplitude, or combinations thereof) of a carrier is varied in accordance with a digital signal.

Digital-to-Analog (D/A) Converter: A device for decoding digital information or turning it into an analog wave form.

Diplexer: A device used to combine two bands.

Dipole: A center fed antenna which is one half wave length long.

Direct Current (DC): Current which flows in only one direction and never changes polarity.

Directional Coupler: A device used to tap off a small part of the signal being transmitted along a coaxial cable while providing high reverse isolation.

Directional couplers are frequently used in coaxial systems for subscriber taps or taking measurements. In wireless, directional wave-guide couplers are used for measuring forward and reflected power at the input to the up-tower transmission line.

Direct Pick-Up Interference (DPI / DPU): Interference picked up on the shield of a coaxial cable connected to a set-top converter box. Also, interference picked up the coaxial input cables of some other communications systems.

Directivity: The degree to which an antenna focuses its power in a specific direction if the antenna were one-hundred percent efficient. Since microwave frequency antennas are highly efficient the difference between gain and directivity is not significant at microwave frequencies.

Discriminator: A specific type of FM detector circuit which senses phase relationships.

Dish: An antenna with a reflector shaped like a bowl. Most so called dish antennas are actually parabolic. See: "Parabolic Antenna" and "Parabola."

Distribution System: The way in which programming is sent to multiple subscribers. In a cable system, the distribution system involves a large network of cables and signal processing amplifiers.

Dolby™: A trade mark name for an audio noise reduction technique frequently used with audio tape involving multi-band pre-emphasis and de-emphasis methods.

Down Converter: A device for lowering the frequency of a modulated radio frequency carrier.

Down Link: Signal coming down from a satellite to a TVRO station.

Down Tilt: A modification of an antenna radiation pattern which focuses energy along a line tilted below the horizontal radiation line. Down tilt uses energy which would other wise be radiated toward the sky or into the ground.

DPI / DPU (Direct Pick Up Interference): See: "Direct Pick Up Interference."

Driver: An amplifier intended to supply enough power or signal level to the input of another power amplifier to drive it.

Drop Line: The coaxial cable connecting a CATV tap to a subscriber's home. Drop lines are usually RG-59 or RG-6 coaxial cables.

Ducting: See: "Microwave Ducting" and "Tropospheric Ducting."

Dummy Load: A load which simulates the input impedance characteristics of another non-reactive device.

E

Earth Station: Usually a TVRO but can also mean an satellite up-link station. See: "Television Receive Only."

Eave Mount: A triangular antenna mounting system used for attaching a mast to the eave or gable of a peaked roof.

Eccosorb®: A trade name for microwave absorber material made by the *Emerson & Cuming Company.*

EEPROM (Electronically Erasable Programmable Read Only Memory): See: "Electrically Erasable Programmable Read Only Memory."

Efficiency: A measure of the degree to which power is used or wasted.

Effective Isotopic Radiated Power (EIRP): See "Equivalent Isotropically Radiated Power."

Effective Radiated Power (ERP): An FCC term for the product of the antenna power input and the antenna power gain expressed in watts.

E Group: See: "Group E."

EHF (Extra High Frequency): See: "Extra High Frequency."

EIRP (Equivalent Isotropically Radiated Power): See: Equivalent Isotropically Radiated Power.

Electro-Motive Force (EMF): See: "Voltage."

Electronically Erasable Programmable Read Only Memory (EEPROM): A form of Read Only Memory which can be rewritten or reprogrammed electrically.

Elevation: A measure of vertical distances or angles.

Elevation Angle: A measure of vertical elevation referenced to the horizontal.

Elevation Beam Width: The vertical measure (usually in degrees) of an antenna pattern.

ELF (Extremely Low Frequency): See: "Extremely Low Frequency."

Elliptical Wave Guide: A semi-flexible corrugated wave guide with an elliptical cross sectional shape. See: "EW-20."

EMF (Electro-Motive Force): See: "Voltage."

Encipher: Use of a cipher process to conceal some form of communicated intelligence.

Enclosure: Usually refers to a headend enclose, relay equipment enclosure hut, or a small weather proof equipment box.

Encode: The process of representing some form of communicated intelligence utilizing a code. See: Code. Sometimes scrambling or security trapping techniques are called encoding. See: Scrambling and Security Trapping.

Encoding: See: "Encode."

Encrypt: See: "Cipher."

Encryption: See: "Cipher and Encipher."

EPROM (Erasable Programmable Read Only Memory): See: "Erasable Programmable Read Only Memory."

Erasable Programmable Read Only Memory (EPROM): A form of Read Only Memory which can be erased with ultraviolet light and reprogrammed.

ERP (Effective Radiated Power): See: "Effective Radiated Power."

Equalizer: See: "Amplitude Equalizer," and "Phase Equalizer."

Equivalent Isotropically Radiated Power (EIRP): An FCC term. The product of the power supplied to the transmitting antenna and the antenna gain in a given direction relative to an isotopic antenna radiator. This product may be expressed in watts or dB above one watt (dBW).

EW-20: A specific size of semi-flexible corrugated wave guide with an elliptical cross sectional shape.

Exa-: A metric prefix which means 1,000,000,000,000,000,000.

External Diplexing: See: "High Level Diplexing."

Extra High Frequency (EHF): Frequencies between 30 and 300 GHz.

Extremely Low Frequency (ELF): Frequencies between 30 and 300 Hz.

F

FAA (Federal Aviation Administration): See: "Federal Aviation Administration."

FAA Advisory Circular AC 70/746-1H: The Federal Aviation Administration Circular which lists current tower marking requirements.

FCC (Federal Communications Commission): See: "Federal Communications Commission."

F Connector: The type of screw on connector used on 75 ohm CATV cable.

Federal Aviation Administration (FAA): The federal regulatory agency responsible for air safety. Establishes tower marking requirements.

Federal Communications Commission (FCC): The federal organization responsible for the regulation of communications utilizing the public air waves in the United States.

Feed: See: "Antenna Feed and Feedhorn."

Feeder Line: A coaxial cable which interconnects a bridger amplifier with various CATV taps within a CATV system.

Feedhorn: The antenna device used for receiving or radiating microwave signals to or from a parabolic dish reflector.

Femto-: A metric prefix which means 1,000,000,000,000,000 or 10^{+15}.

FET (Field Effect Transistor): See: "Field Effect Transistor."

F Group: See: "Group F."

Fiber Optical Cable: A cable which contains optical fibers for the transmission of modulated light signals. Typically an optical cable will contain at least fourteen fibers.

Fiber Modulator: A device which converts RF signals to light for transmission on a fiber optical cable.

Fiber Optics: A transmission system which uses lasers and light to transmit signals through hair like glass optical fibers rather than an electrical conductors. Fiber optics have extremely broad bandwidths.

Fiber Receiver: A device used for demodulating optical signals.

Field Effect Transistor (FET): A transistor which uses electric fields in semi-conductor material to control current flow.

Field Inversion: An analog method of scrambling video involving the inversion of specific video fields.

Filter: A network used for the suppression of certain frequencies or signals.

Filterplexer: See: "Combiner."

Flat Base Mount: A system for mounting a mast on a flat roof using a ground mount plate. See: "Ground Mount."

Flip Flop: A digital device used for storing, processing, or representing bits. It may be triggered or set to either zero or one.

FM (Frequency Modulation): See: "Frequency Modulation."

Foot Print: The broadcast radiation pattern of a satellite transmitter projected onto the earth.

Free Space Loss: The power loss which results when radio frequency energy passes through a vacuum. This kind of power results from the spreading out of radio waves and is sometimes called spreading loss to distinguish it from other losses which occur when radio waves pass through various gasses or material.

Fresnel Zone: A circular area around a microwave path.

Frequency: Number of complete cycles per second usually measured along the x-axis.

Frequency Combiner: A diplexer or frequency splitter used backwards or in reverse.

Frequency Coordinator: A consultant with an up to date FCC database of all licensed transmitters capable of producing computer generated interference simulations and various other propagation studies. See: "Computer Generated Interference Analysis," "Path Study," and "Shadow Map."

Frequency Deviation: The extent to which an FM carrier moves from its center frequency during modulation.

Frequency Drift: The extent to which the unmodulated center frequency of an AM or FM carrier deviates from an FCC assigned frequency.

Frequency Modulation (FM): A method of modulation which varies the frequency of one signal to carry another lower frequency signal.

Frequency Off-Set: An intentional frequency difference between geographically adjacent or semi-adjacent transmitters operating on the same channel or channels. The off-set is typically plus or minus 10 to 12 KHz.

Frequency Response: The output loss or gain of a device or system across a bands of frequencies given a fixed input amplitude.

Frequency Splitter: A device which separates an input band into two output bands. Devices with more than two outputs are also possible. A frequency combiner or diplexer used backwards or in reverse. It takes one band and divides it into two independent bands while suppressing alternate bands.

Frequency Standard: Generally a special receiver which receives synchronized signals transmitted by the *National Bureau of Standards*.

Frequency Tolerance: An FCC term which refers to the degree to which a stations carrier is allowed to be off its assigned frequency.

Front-to-Back Ratio: A measure used to compare the main lobe of an antenna in relation to next strongest lobe of an antenna.

G

Gable Mount: See: "Eave Mount."

Gain: The ratio of the output amplitude of a signal to the input amplitude of a signal. This ratio can be measured as a numerical ratio (numerical gain) or as a decibel radio (dB gain).

Gate: See: "Logic Gate."

Geographic North: North based upon some geographic grid system which may or may not correspond to true north. See: "Grid North."

Geostationary Orbit: See: "Geosynchronous Orbit."

Geosynchronous Orbit: A circular equatorial orbital path approximately 22,247 miles above sea level with an orbital period of approximately 24-hours. The orbital period is synchronized with the earths rotation. Because satellites in such an orbit appear to hang in the sky over the same surface location on earth, the orbit is sometimes called geostationary.

G Group: See: "Group G."

Ghost: A weak television picture mixed with a strong television picture. It may or may not be the similar to the strong picture. A leading or lagging ghost can help a technician determine whether the ghost is caused by a multiple reflection at the antenna, a cable echoes, non-antenna ingress, or direct pick-up interference.

GHz: See: "Gigahertz."

Giga-: A metric prefix meaning one billion or 1,000,000,000.

Gigahertz (GHz): One billion hertz.

Grid North: North based upon some geographical grid system. See: "Geographic North."

Ground: Usually an electrical point of reference arbitrarily chosen as a zero voltage reference point for an electrical circuit. Often the earth itself is chosen as the point of electrical reference. However since the conductivity of the earth varies with location and weather conditions, the earth cannot be considered an absolute point of reference in a universal sense.

Ground Block: A device used to ground the shield of a coaxial cable usually at the point where the cable enters a building.

Ground Bulkhead: A special grounded metal entrance plate to which to the shields of up-tower transmission lines, wave guides, or other up-tower cables are bonded.

Ground Kit: A kit of the parts necessary to ground the shield of a coaxial cable or body of a wave guide to the structure of an antenna tower at periodic

intervals.

Ground Network: The network used to ground electronic equipment. Frequently ground networks for antennas consist of a series of ground rods, radial, and sometimes wire mesh screens buried under the ground around an antenna. See: "Ground Radials."

Ground Mount: A flat plate used for mounting antenna masts on the ground or sometimes on a flat roof.

Ground Noise: Thermal noise emanating from either an electrical ground or from the earth itself.

Ground Radials: Horizontal copper rods or straps buried at the base of an antenna tower to establish an earth ground either for lightning protection or for a propagation plane depending upon the type of antenna being used. See: "Ground Network."

Ground Rod: Usually a six or eight foot copper rod driven into the earth to establish an earth ground.

Ground Strap: A wide copper strap used to ground equipment.

Ground System: The method used to ground electronic equipment. See: "Ground Network."

Ground Wave: Radio wave which propagate along the surface of the earth.

Group A : Four alternate 6 MHz channels between 2.5 and 2.548 GHz.

Group B: Four alternate 6 MHz channels between 2.506 and 2.554 GHz.

Group C: Four alternate 6 MHz channels between 2.548 and 2.596 GHz.

Group D: Four alternate 6 MHz channels between 2.554 and 2.602 GHz.

Group Delay: When two signals of different frequencies pass through a device they may have different propagation delays.

Group E: Four alternate 6 MHz channels between 2.596 and 2.638 GHz.

Group F: Four alternate 6 MHz channels between 2.602 and 2.644 GHz.

Group G: Four alternate 6 MHz channels between 2.638 and 2.686 GHz.

Group H: Four alternate 6 MHz channels between 2.644 and 2.680 GHz.

Guy Wire: Heavy wire cable used for supporting an antenna mast or tower.

GaAs FET: A field effect transistor using Gallium Arsenide as a semiconductor material. Frequently used in transmitter circuits.

H

Hard Encryption: A term used to distinguish more secure digital encryption techniques from less secure analogy scrambling methods.

Harmful Interference: An FCC term for any radiation or induction which endangers the functioning of a radio navigation service or of a safety service or obstructs or repeatedly interrupts a radio service.

Harmonic: A multiple of a specific frequency.

HDTV (High Definition Television): See: "High Definition Television."

Headend: The technical facility of a cable or MMDS system where program processing and distribution equipment is located.

Hecto-: A metric prefix meaning one hundred or 100.

Heliax®: An *Andrew Corporation* trade name for a specific type of coaxial transmission line.

Hertz (Hz): The unit in which cycles are measured (cycles per second).

Heterodyne: A method of beating two signals together in a mixer to produce the sum and difference

of the two frequencies.

Heterodyne Converter: A device consisting of an oscillator and a mixer which beats two signals together for the purpose of down converting or up-converting a modulated carrier.

Heterodyne Channel Converter: A converter which utilizes heterodyne principles to down convert signals on one channel and then re-convert the signals to a new channel. Generally heterodyne converters produce higher quality results than those which utilize frequency multiplication principles. Occasionally the program may be demodulated to a base band frequency (in order to interface with base band encryption equipment) and then re-modulated. Converters often have amplifier, filters, or demodulators, and modulators to boost and clean-up signals. See: "Channel Converter," "Converter, Heterodyne Converter," and "Processor."

Herringbone: Moving or stationary lines superimposed on a television picture.

Hexadecimal: A number system with sixteen symbols (zero to nine and A to F).

HF (High Frequency): See: High Frequency.

H Group: See: "Group H."

High Definition Television (HDTV): Any television system which produces significantly higher resolution pictures than the *NTSC*, *PAL*, or *SECAM* systems.

High Frequency (HF): Frequencies between 3 and 30 MHz.

High Level Combining: A processing of combining channels or carriers at the transmitter outputs.

High Level Diplexing: A processing of combining two radio frequency carriers (usually audio and video) at the final transmitter outputs.

High Level Modulation: Modulation at the last amplifier stage of a transmitter.

Highpass Filter (HPF): device which passes all frequencies above a certain cut off frequency and blocks frequencies below that frequency.

Horizontal Beamwidth: See: "Azimuth Beamwidth."

Hum Bars: Bars caused by power line interference at power line frequencies passing though a television picture.

Hum Modulation: Noise which unintentionally modulates a desired signal frequently at power line frequencies.

Hybrid Coupler: A device with four connectors or two inputs and two outputs which performs the function of a power coupler. One of the outputs is connected to a dummy load impedance to absorb any spurious signals generated in combining process.

Hybrid Splitter: A hybrid coupler used in reverse as as a power splitter. A device with two outputs and two inputs. A dummy load impedance is connected to one of the inputs to "absorb" any reflected power.

Hz (Hertz): See: "Hertz."

I

IF (Intermediate Frequency): See: "Intermediate Frequency."

Image Frequency: The sum or difference of two beat frequencies. Frequently the unused beat frequency in a heterodyne converter.

Impedance: A combination of resistance and (inductive or capacitive) reactance usually measured in ohms. Impedance involves the composite or net opposition to alternating current flow while resistance involves the opposition to both direct current and alternating current flow without a reactive component.

Impedance Matching Network: A network or device for matching one impedance to another. Such devices are typically used to match transmitters to transmission lines or transmission lines to antennas.

Impulse Pay Per View (IPPV): A pay per view system which allows the viewer to use a hand held

control to select a movie for immediate viewing without making a telephone call to order. The fee is charged to the subscriber's bill.

Inclinometer: A device for measuring elevation angles.

Inductance: A property of inductors (measured in Henries) which opposes any change in current flow.

Inductive Reactance: The inductive opposition (measured in ohms) to any change in current flow. This property results from energy in the electro-magnetic field surrounding wires, coils, or other inductors.

Ingress: See: "Non-Antenna Ingress."

Insertion Loss: The loss at desired frequencies resulting from the use of an electronic device. In band loss.

Instructional Television Fixed Service (ITFS): A microwave communications service created by the FCC for the transmission of educational programming between campuses and operated in the 2.5 to 2.686 GHz band.

Interdiction: A method of interdicting pay television channels using addressable taps. See: "Addressable Tap."

Interference: Any undesired man made or natural signal which degrades reception.

Interference Analysis: See: "Computer Generated Interference Analysis."

Intermediate Frequency (IF): A conversion frequency between an original frequency and the final frequency to which it is up-converted or down-converted.

Intermodulation Distortion: Distortion of a wave form caused by the beating of two or more signals together.

Internal Diplexing: Diplexing performed inside a transmitter at some stage prior to the final power amplifiers. See: Low Level Diplexing.

Inverter: See: "Analog Inverter" and "Digital Inverter."

IPPV (Impulse Pay Per View): See: "Impulse Pay Per View."

Isolator: A device with a low forward impedance and a high reverse impedance.

Isotopic Antenna: See: "Isotopic Radiator."

Isotopic Radiator: A theoretical antenna which transmits its power equally in all directions. It is used for comparing real antennas with a theoretically perfect antenna.

ITFS (Instructional Television Fixed Service): See: "Instructional Television Fixed Service."

J

Jack: A receptacle for connecting a wire or cable.

Jumper: A wire or cable with a connector on each end.

K

Key: A list of letters, numbers, symbols, procedures, or an algorithm used in a deciphering process.

Kilo-: A metric prefix meaning one thousand or 1,000.

Kilohertz (KHz): One thousand hertz

Ku Band: The band of frequencies between 15.35 and 17.25 GHz

L

LASER: *Light Amplification by Stimulated Emission of Radiation.* A very narrow highly focused beam of light sometimes used to transmit information.

Latitude: A geographic measure on the surface of the earth measured by the angle north or south of the equator which is usually expressed in either decimal

degrees or degrees, minutes, and seconds.

LF (Low Frequency): See: "Low Frequency."

Lightning Arrester: See: "Lightning Suppressor."

Lightning Suppressor: A device which grounds out surge voltages in order to protect equipment from lightning.

Limiter: A device frequently used in broadcasting for preventing signals from exceeding a specified level in order to prevent over modulation.

Line Extender: A CATV amplifier used on feeder lines for boosting signal levels.

Linear: Having equal divisions. See: "Non-linear" and "Logarithmic."

Line Inversion: An analog method of video scrambling involving the inversion of specific video lines.

Line Shuffle: An analog method of video scrambling involving the transposition of specific video lines.

LNA (Low Noise Amplifier): See: "Low Noise Amplifier."

LNB (Low Noise Block Down Converter): See: "Low Noise Block Converter."

LNC (Low Noise Converter): See: "Low Noise Converter."

Local Oscillator (LO): A device which generates a specific since wave frequency.

Logarithm: An exponent defined by the equation: $x = \text{Log}_n a$ if $n^x = a$.

Logarithmic: A scale having unequal divisions defined by a logarithmic equation. See: "Logarithmic."

Logic: In electronics, the decision making ability of gate circuits. See: "Boolean Algebra."

Logic Gate: A circuit which performs logic operations.

Log Periodic Antenna: An extremely wide band antenna designed with a series of resonate or tuned elements. Typical of many VHF and UHF television antennas.

Log Periodic Antenna Feed: A microwave feed with a log periodic element.

Longitude: A geographic measure of the angle east or west of the prime meridian which is usually expressed in either decimal degrees or degrees, minutes and seconds.

Loop-In: The output of a loop-through.

Loop-Out: The output input of a loop-through.

Loop-Through: A cable or set of jumper cables with connectors which leave a piece of equipment and then re-enters the equipment carrying intermediate frequency signals. A loop-through is usually intended to allow insertion of filters with the equipment.

Low Frequency (LF): Frequencies between 30 and 300 KHz.

Low Level Combining: A process frequently used in multi-channel transmitters for combining channels or carriers at some processing stage prior to the transmitter output.

Low Level Diplexing: A processing of combining two radio frequency carriers (usually audio and video) at some processing stage prior to the final transmitter output.

Low Level Modulation: Modulation at some processing stage prior to the final stage of a transmitter.

Low Noise Amplifier (LNA): A preamplifier designed to minimize the amount of thermal noise introduced into an electronic system.

Low Noise Block Converter (LNB): A pre-amplification device consisting of a low noise

amplifier and a block down converter built into one unit.

Low Noise Converter (LNC): A pre-amplification device consisting of a low noise amplifier and a down converter built into one unit.

Lowpass Filter (LPF): A device which passes frequencies below a certain designated cut off frequency and blocks frequencies above that point.

Low Power Television (LPTV): An FCC designation for low power broadcast television at VHF or UHF frequencies.

LPTV (Low Power Television): See: "Low Power Television."

M

mA: Milliampers.

Magnetic Declination: The difference between true north and magnetic north at a specific point on the earths surface. See: "Declination Diagram."

Magnetic Variation: See: "Magnetic Declination."

Magnetic North: North based upon the magnetic compass or the earths magnetic field.

Mast: A pipe or pole used for mounting antennas.

Master Antenna Television (MATV): A small cable distribution network within a building for distributing programming from a single antenna or set of antennas.

Matching Transformer: See: "Balun," "Impedance Matching Network, and "Transformer."

MATV (Master Antenna Television): See: "Master Antenna Television."

MDS (Multi-point Distribution Service): See: "Multi-point Distribution Service."

MDS 1: The MDS channel defined by the band of frequencies between 2.150 and 2.156 GHz.

MDS 2: The MDS channel defined by the band of frequencies between 2.156 and 2.162 GHz.

MDS 2A: The MDS channel defined by the band of frequencies between 2.156 and 2.160 GHz.

MDU (Multiple Dwelling Unit): See: "Multiple Dwelling Unit."

Medium Frequency (MF): Frequencies between 300 KHz and 3 MHz.

Mega-: A metric prefix meaning one million or 1,000,000 or 10^6.

Megahertz (MHz): One million hertz.

MF (Medium Frequency): See: "Medium Frequency."

Micro-: A metric prefix meaning one millionth or 1/1,000,000 or 10^{-6}.

Microwave: A radio signal in the spectrum above one GHz.

Microwave Absorber: A tuned device used for blocking and preventing or reducing the re-emission or reflection of microwave frequency energy.

Microwave Diffraction: The tendency of microwave radiation to bend around objects.

Microwave Ducting: Under certain conditions the earth and the upper atmosphere or certain layers of the upper atmosphere can sometimes behave as a wave guide with respect to microwave signals carrying them long distances. See: "Tropospheric Ducting."

Microwave Refraction: The bending of microwave signals when they pass through dissimilar media.

Microwave Reflection: The tendency of microwave radiation to bounce off objects and behave according to the physical principles of light.

Mighty-Mount™ : A *Will Norris* trade name for an antenna mounting system which attaches an antenna mast to the back of a pick-up truck either for

temporary site surveys or for a permanent installation.

Milli-: A metric prefix for one thousandth or 1/1,000 or 10^{-3}.

Mixer: A device used to mix or heterodyne two signals.

MMDS (Multi-channel Multi-point Distribution System): See: "Multi-channel Multi-point Distribution System."

Modem: A device used for connecting a computer to telephone lines for the transmission and reception of data by telephone.

Modulation: The process through which a sine wave of one frequency is made to vary according to the variations of another (modulation) frequency or signal. There are many kinds of modulation: amplitude, frequency, and phase, etc.

Modulator: A device for combining audio, video, or data signals with a radio frequency signal so that the radio frequency carriers the other signals.

Monostable Multivibrator (One Shot): A flip flop which changes state when triggered but eventually returns to the original state after a specific period of time.

MSO (Multiple System Operator): See: "Multiple System Operator."

Multi-channel Multi-point Distribution System (MMDS): A microwave communication system operated in the 2.5 to 2.686 GHz band.

Multi-channel Video Program Distributor (MVPD): A broad classification for distributors of multi-channel television programming such as CATV, CCTV, MATV, MDS, and MMDS.

Multi-Channel Transmitter: A transmitter utilizing low level combining techniques to process many channels at the same.

Multipath Reflections: Radio waves from a transmitter which follow a reflected path, rather than a direct path. Frequently these out of phase or time delayed signals create interference or off-set ghosts in a television picture.

Multiplexing: An analog method of compressing one or more communications (or programs) into one channel by interleaving samples of the communications with each other. Digital multiplexing involves similar but more sophisticated combinational processes.

Multi-point Distribution System (MDS): See: "Multi-point Distribution Service."

Multi-point Distribution Service (MDS): An FCC term for a fixed station operating between 2.15 and 2.162 GHz.

Multi-point Grounding: A system of grounding which uses several grounds at periodic intervals. When used with equipment components multi-point grounds can create undesirable ground-loops.

Multiple Dwelling Unit (MDU): An apartment or any household in a multiple dwelling.

Multi-System Operator (MSO): Usually a corporation which owns and operates a variety of cable systems in various localities

Multivibrator: A broad classification for a variety of flip flops. See: Astable Multivibrator, Bistable Multivibrator, Flip Flop, and Monostable Multivibrator,

mV: Millivolts or 10^{-3} volts.

MVPD (Multi-channel Video Program Distributor): See: "Multi-channel Video Program Distributor."

mW: Milliwatts or 10^{-3} watts.

N

NAND Gate: An AND Gate with a digital inverter at its output.

Nano-: A metric prefix meaning one billionth or

1/1,000,000,000 or 10^{-9}.

Nano-second: A unit frequently used to measure time day. One billionth of a second.

National Electrical Code (NEC): A national code establishing electrical standards which has frequently been adopted by incorporation into many local fire codes and ordinances.

N Connector: The type of screw on connector frequently used with fifty ohm coaxial cable.

NEC (National Electrical Code): See: "National Electrical Code."

Negative Trapping: Use of a notch filter, usually in cable system, to trap out part of a signal and thereby deny the signal to non-subscribers.

Noise: Random electrical signals of various frequencies and amplitudes emanating from natural and man made sources.

Noise Figure: The ratio of two signal to noise ratios or the ratio of input and output signal to noise ratios.

Noise Temperature: An amplifier noise rating based upon temperature measured in degrees.

Non-Antenna Ingress: Interference signals which enter a receiver system through some route other than the antenna at intermediate frequencies or on the output channel of a set-top converter box. Such signals can leak into a system by way of the power supply, on the shield of an input cable, through openings in a chassis, or through a poor ground. Remedies include grounding, power line filtering, shielding, or an RF choke on coaxial input lines depending upon the source, route, and cause of the problem. See: "Direct Pick-Up Interference."

Non-Coherent Interference: Any unintelligible television interference such as sparklies, heavy snow, lines in the picture, tearing, or herringbone.

Non-Linear: Having unequal divisions. See: "Linear" and "Logarithmic."

NOR Gate: An OR gate with a digital inverter at its output.

North: See: "Geographic North, Magnetic North," and "True North."

NOT Function: See: "Digital Inverter."

Notch Filter: A narrow band stop filter sometimes called a trap.

NTSC: National Television Standards Committee.

Null Fill: A modification of an antenna radiation intended to fill the null areas in an antenna's usual radiation pattern. Null fill use to cover areas which would otherwise fall into an antenna's null zones.

O

Obstruction Lights: Warning lights mounted on the side of a tower.

Octal: A number system with eight symbols (0 to 7).

Off-Air: Almost universally recognized jargon for over-the-air. More correctly called over the air signals to avoid confusion between on-the-air and off-the-air. See: Over-the-air.

Off-Set Operation: See: "Frequency Off-Set."

OFS (Operational Fixed Station): See: "Operational Fixed Station."

Omni-Directional: To transmit equally at all azimuths.

One Shot: See: "Monostable Multivibrator."

Operational Fixed Station (OFS): A service established by the FCC operating 2.65 and 2.68 GHz).

OR Gate: A digital device which outputs a high state if either or both of its inputs are high.

Orian (Oak Restricted Information and Operation Network): An encryption system developed by *Oak*

Industries.

Oscillator: A device which outputs a certain audio or radio frequency signal .

Over Modulation: Occurs when the level of modulation is so high that the processing amplifiers become saturated. This results in "clipping" or serious distortion of the signal waveform. When a transmitter is over modulated it can cause spurious interference emissions or create harmful interference..

Over-the-Air: Refers to radio or television signals received on a local antenna and processed for re-transmission into a television distribution system.

P

Pad: An impedance coupling used for matching the output of one circuit to the input of another circuit. There are two common types: the L-Pad and the T-Pad. Also a concrete base used for an antenna tower base or TVRO mount.

PAL (Phase Alternate Line) Television: See: "Phase Alternate Line Television."

Panel Antenna: An antenna which consists of a dipole array built in the configuration of a panel.

Parabola: A dish shape defined by a quadratic math function of the form $y = k + a (x - h)^2$. A parabolic shape has the property of reflecting all signals parallel to its axis to a central focal point. See: "Parabolic Antenna."

Parabolic Antenna: A dish like antenna with a parabolic shape which has the ability to focus waves at a single point. Such antennas provide huge power gains and are highly efficient at microwave frequencies. See: "Parabola."

Pass Band: A spectrum of frequencies conducted by an electronic device and usually defined by upper and lower -3 dB points.

Path Loss: The power loss which occur when radio waves move through space along specific path.

Path Profile: See: "Path Study."

Path Study: A scaled cross sectional topographical analysis of a specific propagation path over the earths surface.

Part 17: A section of FCC Rules & Regulations found in the Code of Federal Regulations dealing with tower makings.

Part 21 : A section of FCC Rules & Regulations found in the Code of Federal Regulations dealing with Multi-Point Distribution Service.

Part 73: A section of FCC Rules & Regulations found in the Code of Federal Regulations dealing with broadcast regulations.

Part 74: A section of FCC Rules & Regulations found in the Code of Federal Regulations dealing with ITFS and LPTV.

Part 76: A section of FCC Rules & Regulations dealing with cable television.

Part 94: A section of FCC Rules & Regulations found in the Code of Federal Regulations dealing with Operational Fixed Service.

Pay-Per-View (PPV): A television service which allows viewers to select movies for viewing for a fee which is charged to their bill.

Peak Mount: An antenna mounting system (tripod or ridge mount) used for erecting an antenna at the ridge of roof. See: "Ridge Mount" and "Tripod."

Peak Sync Power: The peak power level of a video envelope measured during the transmission of sync pulses.

Permutation: The process of rearranging a set of elements.

Peta-: A metric prefix which means 1,000,000,000,000,000 or 10^{15}.

Phase Alternate Line (PAL) Television: The television system used in Europe (with the exception

of France).

Phase Locked Loop (PLL): A feed back system used in receivers for locking the phase of a signal to prevent any drift.

Photo Electric Cell: A light activated switch frequently used to turn lights on at dusk or off at sun rise. Sometimes they are also used to dim lights at night.

Pico-: A metric prefix for one trillionth or 1/1,000,000,000,000 or 10^{-12}.

Pipe Mount: An mounting system used for mounting an antenna mast to a vent pipe on a roof.

PLL (Phase Lock Loop): See: "Phase Lock Loop."

Pneumatic Mast: A telescoping mast which is raised and lowered pressurized air..

Polar Plot: A 360-degree graph measuring direction by angle and levels using concentric circles.

Polarization: Refers to the orientation of radio waves emanating from a horizontal or vertical dipole antenna. When radio waves propagate through space their electro-static and electro-magnetic fields are at right to each other and their direction of travel.

Positive Trapping: Use of a notch filter to trap out an interfering carrier inserted in the channel in order to deny service to non-subscribers.

Power Divider: A splitter which divides power from a single input into two or more isolated outputs. Devices with more than two are outputs can also be found.

Power Line Filter: A device which prevents either radio frequency signals or power line surges from passing along a power cable into equipment.

Power Main Surge Protector: A surge suppressor designed for use at the main power box of a building.

Power Splitter: See: "Power Divider"

PPV (Pay-Per-View): See: "Pay-Per-View."

Preamplifier: An amplifier stage which precedes other amplifier stages in order to increase signal amplitudes to a prescribed input level.

Pre-Emphasis: A gradual increase in the amplitude of higher frequency signals prior to modulation in order to improve signal-to-noise ratios. This process is often used in frequency modulation (FM) systems to correct for distortion and noise by emphasizing higher frequency audio signals. Pre-emphasis is also sometimes used in certain video circuits.

Processor: A device which utilizes amplifiers and filters to boost, clean-up and reprocess signals. Sometimes channel converters demodulate signals in order to accomplish this function. See: "Channel Converter."

Propagation: The movement of radio waves through space or along some conductor from a radiator or antenna.

Propagation Delay: The time interval it takes a signals to pass through a device from input to output.

Protected Area: A zone defined by a stations FCC license which is legally protected from interference (on the stations authorized channel or channels) by all other stations.

Pseudo Random: A superficially random process or series of events which really follow some obscure algorithm.

Pseudo Random Number Generator: A device which generates apparently random numbers based upon some algorithm.

Q

QAM (Quadrature Amplitude Modulation): See: "Quadrature Amplitude Modulation."

Quadpod: An antenna mounting system with four legs frequently used for mounting an antenna on the side of a sloped roof. The fourth leg is made using the

antenna mast itself. The system may also be used on other types of roofs for providing additional physical support.

Quadrature: A network designed to produce a phase shift of ninety degrees.

Quadrature Amplitude Modulation (QAM): A method of digital amplitude modulation involving a specific number of discrete states. It can be used to transmit HDTV or several compressed programs in a single 6 MHz channel. 16-QAM has sixteen discrete states while 64-QAM has sixty-four discrete states.

R

Radials: See: "Ground Radials."

Radiation Pattern: The propagation characteristics of an antenna.

Radio Frequency (RF): The range of frequencies in the electromagnetic spectrum from 3 KHz to 300 GHz.

Radio Horizon: Because radio waves tend to bend over the horizon the radio horizon is further away than the visual horizon. Radio horizon calculations are based upon an imaginary earth which is 4/3rds the size of the real earth.

RAM (Random Access Memory): See: "Random Access Memory."

Random: Without predictable pattern or any known algorithm.

Random Access Memory (RAM): A system for retrieving computer files from a digital storage system without reading any other files.

Random Number Generator: A device which generates random numbers without following any known algorithm. See: "Pseudo Random Number Generator."

Range Finder: A device for optically measuring the range to an object.

Ratio Detector: A specific type of FM detection circuit which uses principles similar to a discriminator but provides some amplitude limiting.

Reactance: An inductive or capacitive opposition to any change in current flow measured in ohms. See: "Capacitive Reactance" and "Inductive Reactance."

Read Only Memory (ROM): A digital storage system which may be read but not altered under normal operational circumstances.

Refraction: See: "Microwave Refraction."

Reflection: See: "Microwave Reflection."

Relay: A station which receives signals and rebroadcasts them either on the same frequency or on a different frequency. See: "Repeater," "Signal Booster," and "Translator."

Repeater: A relay which re-transmits signals received on one antenna from another antenna for the purposes of extending the range or distribution pattern of the original transmission.

Resistance: The opposition to current flow in conductors measured in ohms.

Return Loss: A measure of reflected power.

RF (Radio Frequency): See: "Radio Frequency."

RF Modulator: See: "Modulator."

RG-6: A type of 75-ohm cable (larger than RG-59).

RG-8: A type of 50-ohm cable (larger than RG-58).

RG-58: A type of 50-ohm cable (smaller than RG-8).

RG-59: A type of 75-ohm cable (smaller than RG-6).

Ridge Mount: An antenna mounting device used for connecting a mast to the ridge of roof.

ROM (Read Only Memory): See: "Read Only Memory."

S

S/N (Signal-to-Noise Ratio): See: Signal-to-Noise Ratio.

Satellite Master Antenna Television (SMATV): A small cable distribution network within a building for distributing programming from one or more central satellite receiver antennas.

SAW (Surface Acoustical Wave) Filter: See: "Surface Acoustical Wave Filter."

SCC (System Control Computer): See: "System Control Computer."

Scramble: See: "Scrambling."

Scrambling: Traditionally defined in the science of cryptology as an analog method of concealing communications signals which utilizes the processes of heterodyne, band division, transposition, reversal, or inversion. Sometimes use of positive tapping is called scrambling. See: "Positive Trapping."

SECAM (Sequential a Memoire) Television System: The television system used in France.

Selectivity: The ability of a circuit to pick up a narrow band of frequencies while rejecting adjacent frequencies.

Sensitivity: The ability of circuit to pick up weak signals.

Screen: A wire mesh device or shield used for blocking radio frequency energy.

Second Order Harmonics: The second multiple of a specific frequency or a specific frequency multiplied by two.

Sectional Parabolic Antenna: A parabolic antenna which consists of only a slice or part of a complete parabolic dish.

Security Trapping: See: "Positive Trapping," and "Negative Trapping."

Security: See: "Scrambling," "Cipher," and "Code."

Set-Top Converter Box: The converter box which sits on top of the TV set for receiving CATV or MMDS TV. See: "Subscriber Converter."

Semi-Adjacent Channel: A channel separated from specific channel by one channel.

Shadow Map: A map generated either from computer simulations or an actual area survey showing terrain blockage with respect to a specific radio transmitter.

SHF (Super High Frequency): See: "Super High Frequency. "

Shield: Any solid or wire mesh device used to block radio frequency energy. See: "Screen" and "Microwave Absorber."

Shift Register: A digital counter like device which shifts bits to the right or left frequently used in computers and advanced digital encryption equipment.

Shroud: See: "Antenna Shroud."

Siamese Cable: Two coaxial cables manufactured in pairs with a connecting web between the cables much like the web used on 300-ohm twin lead.

Side Band: A lower or higher frequency signal which is created when one signal is used to modulate another signal. The band of frequencies to the right or left of a channels center frequency.

Side Lobe: A minor lobe of an antenna pattern as distinguished from the main lobe(s) of an antenna pattern.

Signal Bender: See: "Signal Booster" and "Beam Bender."

Signal Booster: By FCC definition a signal booster is a low power relay or repeater.

Signal-to-Noise Ratio (S/N): The ratio of the amplitude of a specified signal to the amplitude of background noise. The signal could be either an audio

signal or a radio frequency signal. S/N is a broader measure than C/N because it includes audio frequencies. However, at radio frequencies the desired signal is more properly called a carrier to avoid confusion between the carrier and any signals modulated on the carrier.

Single Channel Transmitter: A transmitter used to process only one television channel.

Single Point Ground: A system of grounding which terminates all grounds at one ground point.

Single Side Band (SSB): A form of amplitude modulated transmission which broadcasts only one set of sidebands rather than two sets of sidebands (upper sidebands and lower sidebands). For a given composite power output, an SSB transmission has the effect of being much more powerful than a regular AM transmission because unnecessary power is not wasted in a redundant set of sidebands. There are two forms of SSB transmission - (1) regular SSB, and (2) SSB suppressed carrier. The former format includes the original carrier. The later format suppresses or eliminates the original carrier and broadcasts only the sidebands. With SSB suppressed carrier formats, the carrier is restored at the receiver using an oscillator for reception.

Site Survey: An on-location evaluation using test and other forms of equipment. There are at least four kinds of site surveys: (1) installation or so called proofing surveys; (2) isolation surveys; (3) area or coverage surveys; and (4) interference surveys.

Skin Effect: The tendency of high frequency radio signals to propagate toward the surface of a conductor rather than in its core.

Sky Wave: Radio signals propagate through the upper atmosphere as opposed to along the ground. See: "Ground Wave."

Slope: The ratio of the rise to the run of a line. In communication electronics slope usually refers to the slope of an amplifier curve.

Slot Antenna: An antenna composed of a dipole across a slot shaped aperture.

SMART Card: A card which contains an algorithm , cryptographic key, or a microprocessor for use with decryption equipment.

SMATV (Satellite Master Antenna Television): See: "Satellite Master Antenna Television."

Snow: Heavy sparklies in a television picture frequently caused by noise when signal levels are low or by strong terrestrial interference when desired signal levels are high.

Sparklies: Small stars in a television picture which result from interference.

Spectrum: A continuous range of frequencies defined by some upper and lower limits.

Splitter: A device which divides an input into two or more isolated outputs. See: "Power Divider" and "Frequency Splitter."

Spurious Signals: Undesired interference.

Spreading Loss: See: "Free Space Loss."

SSB (Single Side Band): See: Single Side Band.

Standing Wave Ratio (SWR): The ratio of power to reflected power in a radio frequency device.

STL (Studio-to-Transmitter Link): See: "Studio-to-Transmitter Link."

Stop Band: A spectrum of frequencies blocked by an electronic (filter) device and usually defined by upper and lower - 3 dB points.

Strobe: A high intensity flasher frequently used as a warning light.

Studio-to-Transmitter Link (STL): A microwave link used for transporting programs from a studio to a transmitter.

STV (Subscription Television): See: "Subscriber Television."

Subscriber Converter: The converter box (usually on

top of a subscriber's television set) which down converts signals for input to the subscriber's television.

Subscriber Tap: A device used to take a small portion of signal off a cable and feed it to a subscriber.

Subscriber Television (STV): Television in which the subscribers pay a fee for programming as compared with commercial television where they do not.

Subscription Television: See: "Subscriber Television."

Sub-Band: The band of frequencies between 5 MHz and 45 MHz frequently used as a return path in CATV.

Super High Frequency (SHF): Frequencies between 3 and 30 GHz.

Superflex®: An *Andrew Corporation* trade name for a specific type of their flexible coaxial transmission line.

Surface Acoustical Wave (SAW) Filter: A specific type filter made of piezoelectric material.

Surge Suppressor: A device which grounds out surge voltages to protect equipment from either power line surges or lightning surges.

SWR (Standing Wave Ratio): See: "Standing Wave Ratio."

Sync Inversion: An analog method of scrambling video involving the inversion of sync pulses.

Sync Pulse: A pulse used to synchronize a signal. In television sync pulses are used to synchronize frames in the picture.

Sync Removal and Replacement: An analog method of scrambling video involving the removal of sync pulses.

Sync Suppression: An analog method of scrambling involving the suppression of sync pulses.

System Control Computer (SCC): The computer system used at CATV or MMDS headend for control of numerous technical functions. These functions include subscriber addressing, channel mapping schedules, ad insertion, encryption keys, PPV, and sometimes IPPV.

T

Tap: A device used to take a small proportion of signal off a cable for feeding a drop line to subscriber's home. CATV taps at are usually made using directional couplers and balanced power dividers. Typically taps have four, six, or eight drop line outputs.

Tearing: A television picture interference pattern which characterized by a broken or torn picture.

Telco: An abbreviation for "Telephone Company."

Television Receive Only (TVRO): An earth station designed to receive satellite transmissions.

Temperature Compensation: An equipment option which prevents an RF circuits from changing frequency as a result of temperature changes. As components change temperature they expand or contract. This can cause them to change value.

Tera-: A metric prefix meaning one million or 1,000,000,000,000 or 10^{12}.

Terminator: A load used on an output in order to - (1) prevent the radiation of signals from an output, and (2) maintain the impedance balance of an electronic device.

Terrestrial Interference (TI): Interference emanating from sources on the earth as contra-distinguished from those emanating in space.

Thermal Noise: Noise resulting from the movement of sub-atomic particles. Such noise is a function of temperature.

Third Order Harmonics: The third multiple of a specific frequency or a specific frequency multiplied by three.

Tie Wrap: A plastic band used for bundling or harnessing cables together.

Tier: A number of television channels sold together as a group.

Tier Filter: A negative broadband stop filter used for block a spectrum of television channels from non-subscribers.

TI (Terrestrial Interference): See: "Terrestrial Interference."

Timing: Clock pulses used to synchronize circuit operation.

TOCOM: A General Instrument encryption system similar to Z-TAC.

Topographical Map: A type of relief map which represents land features using concentric lines.

Tower: A structure used for mounting antennas. Towers may be classified in many ways: by (1) mounting system (self supporting or guyed); (2) shape (triangular, square, or pole); (3) erection method (crank-up; tilt-over; or erected sectionals); and (4) weight and height (heavy or light).

Tower Marking: Tower lighting or painting with specific patterns so that the tower can be easily seen by aircraft pilots.

Transformer: A device used to step up or step down either voltage or impedance. Transformers are also sometimes used simply to isolate two circuits from each other.

Transistor-Transistor Logic (TTL): A type of integrated logic circuit made using bipolar junction transistors.

Translator: A radio relay which receives signals on one frequency and converts them to another frequency for rebroadcast.

Transmission Line: A coaxial cable or wave guide used for connecting a transmitter to an antenna.

Transmission Pattern: See: "Radiation Pattern."

Transfer Switch: Usually a switch which reverses two input-output combinations.

Transportation System: In CATV the transportation system refers to the system used for transporting signals from a remote headend to a main headend. It may also refer to the system used for importing out-of-town signals. CATV transportation systems usually consist of an amplitude modulated microwave link or a fiber optical line.

Trap: See: "Notch Filter," "Positive Trapping," and "Negative Trapping."

Triple Beat: Odd order intermodulation resulting from three carriers beating together.

Tripod: A three legged mounting system used for mounting antenna masts to different structures including ridged roofs and flat roofs.

Troposphere Ducting: When the troposphere layer of the upper atmosphere acts as a wave guide propagating radio signals long distances.

True North: North based upon the earths axis which points to the star Polaris.

Trunk Amplifier: A CATV amplifier used for boosting signals on CATV trunk lines. Trunk amplifiers typically contain automatic slope controls, automatic level controls, equalization circuits, and power supplies.

Trunk Line: A main coaxial cable line connecting a CATV headend with various feeder lines with a CATV system.

TTL (Transistor-Transistor Logic): See: "Transistor-Transistor Logic."

Turnbuckle: A device used for tightening the tension on guy wires.

Tuned Absorber Shield: See: "Microwave Absorber."

TVRO (Television Receive Only): See: "Television Receive Only."

Type Acceptance: An FCC equipment certification procedure.

Type Approval: An FCC equipment certification procedure involving equipment lab tests.

Type BNC Connector: See: "BNC Connector."

Type F Connector: See: "F Connector."

Type N Connector: See: "N Connector."

U

UHF (Ultra High Frequency): See: "Ultra High Frequency."

Ultra High Frequency (UHF): Frequencies between 300 MHz and 3 GHz.

Up Converter: A device which converts signals to a higher frequency.

Up Link: Usually signals transmitted from an earth station to a satellite.

V

VC (VideoCipher) II: See: "VideoCipher II."

Venetian Bind Effect: A television screen interference pattern which looks like venetian blinds.

Very High Frequency (VHF): Frequencies between 30 and 300 MHz.

Very Low Frequency (VLF): Frequencies between 3 and 30 KHz.

Vertical Beamwidth: See: "Elevation Beamwidth."

Vestigial Side Band (VSB): An amplitude modulated format which involves broadcasting only one set of sidebands. See: Single Side Band.

VF (Voice Frequency): See: "Voice Frequency."

VHF (Very High Frequency): See: "Very High Frequency."

Video: Television picture signals.

VideoCipher (VC) II: An encryption system belonging to *M/A COM.*

VideoCrypt: A French encryption system created by the *Thompson Company.*

Video Modulator: A device used to place video information on higher frequency signals for transmission.

Video Signal: The signal which carries the intelligence necessary to make a television picture.

VLF (Very Low Frequency): See: "Very Low Frequency."

Voice Frequency: Frequencies between 300 Hz and 3 KHz.

Voltage: A difference of potential or electric charge between two electrodes sometimes called electo-motive force. When one electrode has more electrons than another a difference of potential is said exist between the two.

Voltage Standing Wave Ratio (VSWR): The radio of voltage to reflected voltage in a radio frequency device.

Voltage Tuned Oscillator (VTO): An oscillator whose frequency is tuned by means of a voltage level.

Vestigial Side Band Modulation (VBS): A form of amplitude modulation using one complete sideband and only part of the other side band.

VSB (Vestigial Side Band): See "Vestigial Side Band."

VSWR (Voltage Standing Wave Ratio): See: "Voltage Standing Wave Ratio."

VTO (Voltage Tuned Oscillator): See: "Voltage Tuned Oscillator."

W

Wall Mount: A Mounting system used for attaching an antenna mast to a building wall.

Waveguide: A conduit or pipe like transmission line used for carrying microwave frequency radio waves.

Waveguide Adapter: A device for adapting signals on a coaxial cable to wave guide or the opposite.

Waveguide Bridge: A roof like structure mounted over a transmission line between a transmitter enclosure and a tower. It keeps snow and ice from forming on the transmission line and protects the line from falling ice.

Waveguide Cut-Off Frequency: The lowest frequency which a wave guide can handle.

Waveguide Flange: A mechanical connector for joining wave guide sections.

Waveguide Switch: A transmission line switch which utilizes a shutter to open or block an aperture in order block or pass radio frequency energy.

Wave Length: The length of one complete cycle of a wave often measured. in terms of distance (meters) or time (seconds). One complete cycle of a wave form which repeats itself.

Windshield Wiper Effect: A television picture interference pattern characterized by a vertical bar which sweeps across the screen.

Wipeout: A completely blank television screen caused by extremely strong interference.

Wireless Cable: Slang jargon for multi-channel television broadcasting.

Wireless MATV (WMATV) System: A coaxial distribution network which receives television programming from a wireless receiver.

Wire Wrap: See: "Tie Wrap."

WMATV (Wireless Master Antenna Television) System: See: "Wireless MATV System."

WR-340: A specific size of rigid waveguide with a rectangular cross sectional shape and a width of 3.4 inches.

WR-430: A specific size of rigid waveguide with a rectangular cross sectional shape and a width of 4.3 inches.

X

XOR Gate: A digital device which outputs a high state only if either of its inputs are high (but not both).

Y

Yagi Antenna: An antenna system which employs a basic antenna element with parasitic reflector and director elements in order to achieve highly directional characteristics.

Z

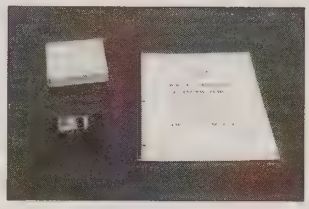
Z-TAC: An Pay Per View system created by *Zenith.*

OTHER BOOKS AVAILABLE FROM C&E

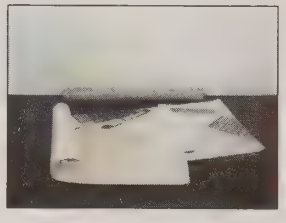
Books on MMDS "Wireless TV"

WIRELESS "PROOFING" SURVEYS
BOOK # B-018

The MMDS Wireless Cable Installation Manual
Book # B-017



A GLOSSARY OF WIRELESS (MMDS/ITFS) TELEVISION TERMS
BOOK # B-011

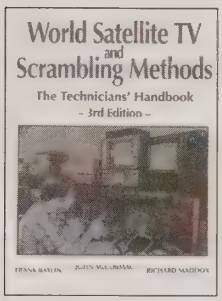


WIRELESS HEADEND PLANS
BOOK # B-013

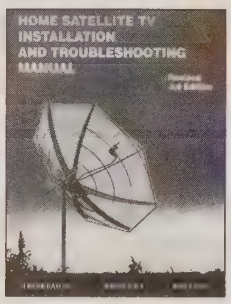
THE WIRELESS PRIMER
BOOK # B-014

Reach us by email: books@cefilter.com

Other Cable & Satellite Titles



WORLD SATELLITE TV AND SCRAMBLING METHODS
BOOK # B-015



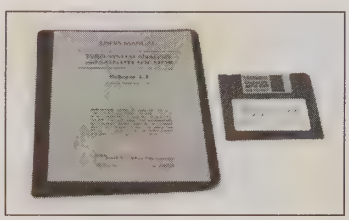
HOME SATELLITE TV INSTALLATION AND TROUBLESHOOTING MANUAL
BOOK # B-008

HOME SATELLITE TELEVISION VIDEO TAPE
BOOK # T-001

THE HIDDEN SIGNALS ON SATELLITE TV
BOOK # B-005

KU-BAND SATELLITE TV
BOOK # B-007

SATELLITE DEALER'S SUCCESS GUIDE
BOOK # B-006

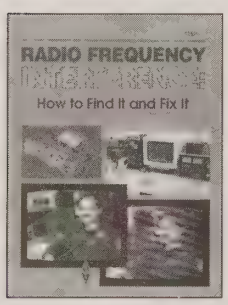


TVRO SYSTEM ANALYSIS AND SATELLITE LOCATOR
BOOK # D-002

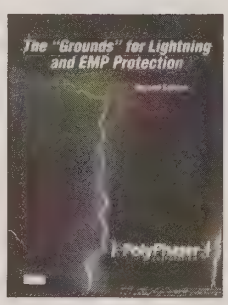
WIRELESS CABLE & SMATV
BOOK # B-003

Order by Book Number • Request our Book Catalog

Interference



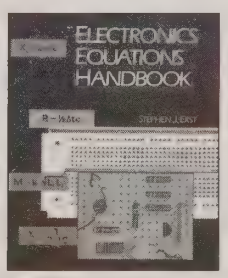
RADIO FREQUENCY INTERFERENCE
BOOK# B-012



THE "GROUNDS" FOR LIGHTNING AND EMP PROTECTION
BOOK # B-010

Engineering

INTERNATIONAL CONVERSION CHART HANDBOOK
BOOK # B-019



ELECTRONICS EQUATIONS HANDBOOK
BOOK # B-016

Communications & Energy Corporation • 7395 Taft Park Drive • East Syracuse, New York 13057
Tel 315-452-0709 • (800-882-1587 US/CAN) • Fax 315-452-0732

Toll free: 800-628-0088
Fax # 817-280-0745
www.spectrummhz.com

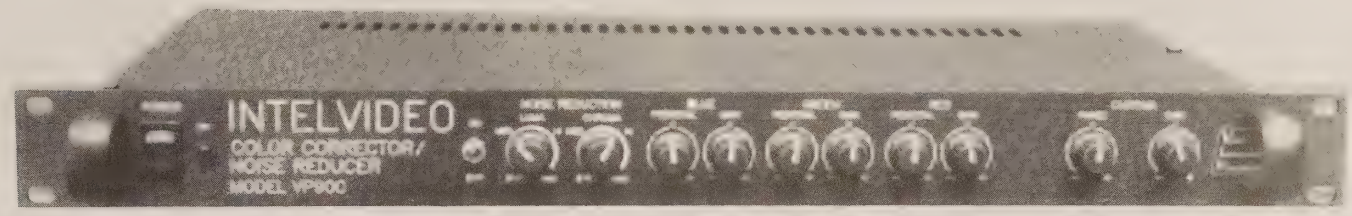
SPECTRUM

"SOLUTIONS" Not Just Products...

Intelvideo INC.

VIDEO IMPROVEMENT PROCESSOR

NTSC COLOR CORRECTOR MODEL VP900 *(For Positive Scrambled Channels)*



DESCRIPTION:

Intelvideo's NTSC Color Corrector Model VP900 goes to the root of color errors and provides the means to truly apply the proper correction.

Conventional color correctors are able to modify chroma phase and color saturation, but changing chroma phase and saturation independent of luminance gain and black level results in a violation of the constant luminance principle, i.e., in luminance errors. The Model VP900 provides not only chroma phase and gain adjustment but by incorporating the circuits of the Model VP700 Decoder, it also gives full control of amplitude and pedestal for each primary color, permitting full color balance of highlights as well as low lights.

The VP900 features Intelvideo's VIP technology. The VIP engine (Video Improvement Processor) is a proprietary system that utilizes recursive filtering techniques with motion compensation to provide over 9 dB's of random noise reduction in both luminance and chrominance. Independent noise reduction of Y and C permits system optimization for different types of random noise, e.g. "snow," color streaks, beats and other random interference.

We also carry the full line of Communications & Energy Products!

SPECIFICATIONS:

INPUT: NTSC color signal
1v pp into 75 Ohms with loop through
OUTPUTS: Two NTSC color signals, 1v pp into 75 Ohms
Optional Outputs: Red, Blue, Green baseband signals

CONTROL FUNCTIONS:
Red Gain: 0 to 140%
Red Pedestal: ±20%
Blue Gain: 0 to 140%
Blue Pedestal: ±20%
Green Gain: 0 to 140%
Green Pedestal: ± 20%
Chroma Gain: ± 20%
Chroma Phase: ± 20°

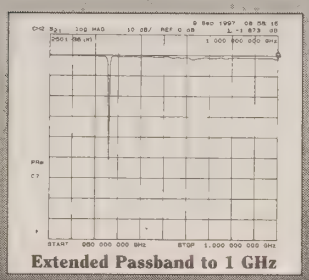
LUMINANCE NOISE REDUCTION: 0dB to 9dB of noise reduction (motion and initial picture quality dependent)
CHROMINANCE NOISE REDUCTION: 0dB to 9dB (motion and initial picture quality dependent)
VIDEO SPECIFICATIONS:
Frequency Response: +.5dB to 5 MHZ
Differential Gain Errors: <2% plus quantizing effects
Differential Phase Errors: <1° plus quantizing effects
K Factor with 2T Pulse: Better than 1%
Frame Tilt: Less than 2%
S/N: >50dB
System Delay: 2 µs plus 1 TV line nominal
POWER REQUIREMENTS: 115 volts 60 Hz, 25 Watts
OPERATING TEMPERATURE: 40° F to 105°F, Ambient
HUMIDITY: 10% to 90% non-condensing
MECHANICAL: 1RU cabinet; 1.75" H, 19" W, 11" L; 7 Lbs

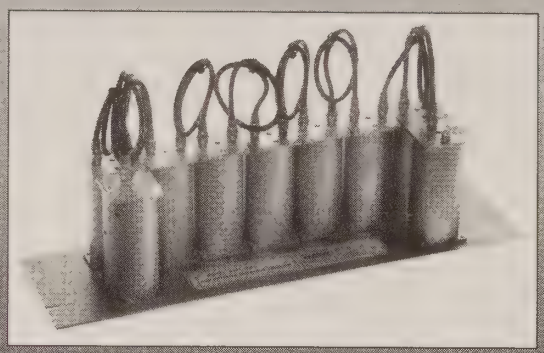
Specifications subject to change without notice 9/96.

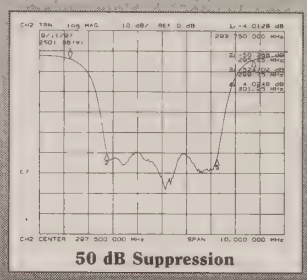
CHANNEL DELETION FILTERS!

- **Channels 2 to 36**
- **Competitive Pricing**
- **Special Frequencies & Options Available**

Emily Bostick - Continuing service to TV Industries WORLDWIDE!


Extended Passband to 1 GHz




50 dB Suppression

Emily Bostick
President

Emily Bostick

EEEEEEE
COMMUNICATIONS & ENERGY CORP

BOSTICK FILTER DIVISION
Tel: (315) 452-0709
Fax: (315) 452-0732

E-MAIL (Sales): sales@cefilter.com
E-MAIL (Technical): tech@cefilter.com
WEBSITE: http://www.cefilter.com

7395 TAFT PARK DRIVE • EAST SYRACUSE, NY 13057 • CANADA & US: 800-882-1587

YOUR ADVERTISEMENT COULD BE HERE !

... in our next publication or reprint in black and white or full color.

Are you a Manufacturer? System Integrator? Consultant?

If your company sells products or services in any of these markets:

CATV
LPTV
PRIVATE CABLE
SATELLITE RECEPTION
MMDS

The Electric Press would be happy to reserve advertising space for you in our next reprint or new publication. If you don't have a current ad, we'll completely lay one out for you from your written copy and supplied photos.

Don't miss the chance to advertise in these publications:

The Wireless Primer

Wireless "Proofing" Surveys

Trapping in CATV

For advertising rates and publication schedules, please contact:

Daniel Bostick or Ronald Mohar at 800 - 882 - 1587

Call to Authors...

Do you have a book in you?

The Electric Press (Division of Communications & Energy Corp.) specializes in working with hands-on engineers and technicians to bring to press "how-to" books covering all aspects of TV broadcast delivery, reception and distribution, such as:

- **CATV**
- **LPTV**
- **MMDS**
- **PRIVATE CABLE**
- **SATELLITE RECEPTION**

Our editors will work with you to bring your manuscript to publication to produce royalties for you, or they will work with you to develop a book out of your experience.

So, if you have something to tell your fellow professionals in any of the above areas, just call us to talk it over.

Call...

Daniel Bostick (315) 452-5488 or

Ronald Mohar (315) 452-0709

enuator cleans up the noise in your return path. Our new Step Attenuator cleans up the noise in your re

Our new Step Attenuator cleans up the noise in your return path.

High-speed data transmission over the return path is your gold mine for the 21st century – but only if you can provide reliable, downtime-free service. Our new Step Attenuator* provides the flexibility for services you need today and in the future. And with our full complement of Mini High Pass Filters and Window High Pass Filters, we offer unparalleled solutions to your return path challenges.

These proven Arcom innovations will help eliminate ingress, balance the return signals, drop the noise floor and make sure only desired information gets transmitted – without any interference.

Arcom return filters are quickly becoming essential for any operator who wants to compete in this emerging market. For complete specs and details, call today.

ARCOM

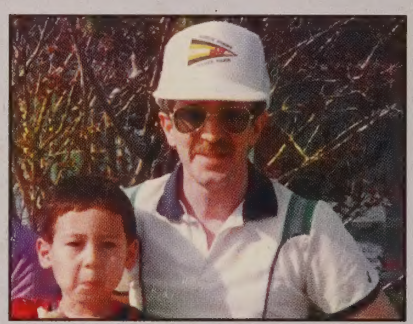
185 Ainsley Dr., PO Box 6729, Syracuse, NY 13210
(315) 422-1230 • (800) 448-1655 • Fax: (315) 422-2963

*Patent pending

CATV TRAPPING
Security Filtering for Pay Television

By Glyn Bostick, Emily Bostick, and Ronald E. Mohar

Every month CATV trade magazines and newsletters report increasing levels of cable television piracy. Unfortunately, some of the most sophisticated program security systems have proven to be *seriously flawed*. Although pay television filtering is the oldest program security method, ***CATV "Trapping"*** is the first book to systematically explain the applications of this "tried and true" technology. The book begins by explaining the history and origins of both pay television and pay television filtering technology. Before explaining the technical operation of positive filtering, negative filtering, single channel filtering, and tier filtering, the book compares pay filtering technology with a variety of other security systems and analyzes the strengths and weaknesses of each. ***CATV "Trapping"*** then discusses the *economics of filtering* and shows you how to use pay television filtering in conjunction with other methods in order to enhance the security provided by other systems. The book also discusses system audits, cable piracy, the properties of a good encryption system, and specialized filtering technology. ***CATV "Trapping"*** is *fully documented* with *authoritative bibliographical sources*. The book includes an appendix and a glossary of technical terms.



Glyn Bostick, BSEE
(1923-1997)

Mr. Bostick Co-founded *Communications & Energy Corporation* and served as its Executive Vice President from its inception. He graduated from Yale in 1947. During his first employment at *Airborne Instrument Laboratories*, he was trained by many of the engineers and scientists who pioneered the use of high frequency and microwave frequency radio technology during World War II. During the last fifty years he has worked as a design engineer with a variety of firms including *General Electric*, *Grumman Aircraft*, and *Westinghouse*. He wrote a variety of books and articles on TVRO, CATV, LPTV, MMDS, and RF filtering technology. In 1967 he founded *Microwave Filter Company (MFC)* with his wife Emily. He served as President and Chief Engineer of *MFC* until 1992. Mr. Bostick maintained no business connection with *MFC*.

Emily Bostick is president and co-founder of *Communications & Energy Corporation*. In 1967 she co-founded *Microwave Filter Company* with her husband Glyn. Between 1967 and 1992 she served as executive vice-president and director of marketing for *Microwave Filter Company*. During the formative years of the cable television industry- when most CATV systems were rural "mom and pop" operations- Emily was among the first to recognize cable television as a significant market. When C-Band satellite broadcasting revolutionized television, Emily introduced cable and television broadcasters to many of the interference control filters which are standard products today. Since that time, she has worked to introduce these products to operators throughout the world. Currently Mrs. Bostick has no business connection with *MFC*.

Ronald E. Mohar, MS

(pictured with his son Edward) is director of technical publishing and market research with *Communications & Energy Corporation*. He graduated from *Syracuse University* and is an FCC Licensed Radiotelephone Operator. He has written a variety of books and articles on CATV, MMDS, and LPTV technology. A graduate of the U.S. Army Signal Center & School at Fort Monmouth, N.J., Mr. Mohar served with the *U.S. Army Communications Command - Europe* in the field of Communications Security. He subsequently worked for the *Board of Cooperative Educational Services (BOCES)* as a technical instructor, and with *Microwave Filter Company*. Mr. Mohar holds a New York State Teaching Certificate and currently serves as an adjunct instructor with *Jamesville-DeWitt Central Schools* and *Fayetteville-Manlius Central Schools* near Syracuse.

© 1997 EPNY div. C&E Corp.
ISBN: 1-888552-07-7